

**CHARTING A PATH FORWARD: THE HOMELAND  
SECURITY DEPARTMENT'S QUADRENNIAL  
HOMELAND SECURITY REVIEW AND  
BOTTOM-UP REVIEW**

---

**HEARING**

BEFORE THE

**COMMITTEE ON  
HOMELAND SECURITY AND  
GOVERNMENTAL AFFAIRS  
UNITED STATES SENATE**

**ONE HUNDRED ELEVENTH CONGRESS**

**SECOND SESSION**

**JULY 21, 2010**

Available via the World Wide Web: <http://www.fdsys.gov/>

Printed for the use of the Committee on Homeland Security  
and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

58-402 PDF

WASHINGTON : 2011

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TOM COBURN, Oklahoma
THOMAS R. CARPER, Delaware	SCOTT P. BROWN, Massachusetts
MARK L. PRYOR, Arkansas	JOHN McCain, Arizona
MARY L. LANDRIEU, Louisiana	GEORGE V. VOINOVICH, Ohio
CLAIRE McCASKILL, Missouri	JOHN ENSIGN, Nevada
JON TESTER, Montana	LINDSEY GRAHAM, South Carolina
ROLAND W. BURRIS, Illinois	
EDWARD E. KAUFMAN, Delaware	

MICHAEL L. ALEXANDER, *Staff Director*

BETH M. GROSSMAN, *Senior Counsel*

TROY H. CRIBB, *Counsel*

CHRISTIAN J. BECKNER, *Professional Staff Member*

BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*

ROBERT L. STRAYER, *Minority Director for Homeland Security Affairs*

LUKE P. BELLOCCHI, *Minority Counsel*

DEVIN F. O'BRIEN, *Minority Professional Staff Member*

TRINA DRIESSNACK TYRER, *Chief Clerk*

PATRICIA R. HOGAN, *Publications Clerk and GPO Detailee*

LAURA W. KILBRIDE, *Hearing Clerk*

## CONTENTS

---

Opening statements:	Page
Senator Lieberman .....	1
Senator Collins .....	4
Senator Voinovich .....	11
Senator Brown .....	15
Senator McCain .....	21
Prepared statements:	
Senator Lieberman .....	27
Senator Collins .....	30

### WITNESS

WEDNESDAY, JULY 21, 2010

Hon. Jane Holl Lute, Deputy Secretary, U.S. Department of Homeland Security	
Testimony .....	6
Prepared statement .....	33
Responses to post-hearing questions for the Record .....	44

### APPENDIX

Department of Homeland Security report titled "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," February 2010 .....	95
Department of Homeland Security report titled "Bottom-Up Review Report," July 2010 .....	202





**CHARTING A PATH FORWARD:  
THE HOMELAND SECURITY DEPARTMENT'S  
QUADRENNIAL HOMELAND SECURITY  
REVIEW AND BOTTOM-UP REVIEW**

---

**WEDNESDAY, JULY 21, 2010**

U.S. SENATE,  
COMMITTEE ON HOMELAND SECURITY AND  
GOVERNMENTAL AFFAIRS,  
*Washington, DC.*

The Committee met, pursuant to notice, at 10:06 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Kaufman, Collins, Brown, McCain, and Voinovich.

**OPENING STATEMENT OF CHAIRMAN LIEBERMAN**

Chairman LIEBERMAN. The hearing will come to order. Thanks very much to everyone for being here. In particular, welcome, of course, to the Deputy Secretary of the Department of Homeland Security (DHS), Jane Holl Lute.

In the 9/11 Recommendations Act of 2007, Congress mandated that the DHS carry out a Quadrennial Homeland Security Review (QHSR) as a way to develop and update strategies for homeland security within the Federal Government and ensure that the Department's programs and activities were aligned with that homeland security strategy. The Act required that the initial QHSR be provided to Congress by the end of 2009.

The QHSR was modeled on the Quadrennial Defense Review (QDR) that was put in place in the 1990s to ensure that the leaders of the U.S. military would focus on emerging national security threats, that to some extent the requirement to do the QDR would force them to look above the pressing events of the day, over the horizon to the challenges that were ahead, and then to develop and present to Congress and the public the strategies and resources to counter them.

The QHSR report, which was completed in early February, and the follow-on Bottom-Up Review (BUR) report, which was completed and issued just a few weeks ago, are meant to serve the same purpose for homeland security. They have the potential, I think, to be the catalyst for ongoing transformation and improvement of the Department, as well as across our entire homeland security community outside of the Department, and in that sense, we

are very fortunate to have Ms. Lute with us because I know that she oversaw these two reports.

This morning we want to hear about the results of the process, including the impact that it is having on strategic planning more broadly within the Department and at other homeland security agencies.

I would like to hear about the steps that will be taken to implement the initiatives described in the BUR report, including how it will impact the Department's budget priorities in future years and how the Department intends to work with Congress on initiatives that may require statutory changes.

Forty-four initiatives are described in the BUR report, in areas such as information sharing, management integration, DHS regional alignment, and the organizational framework for cybersecurity. In fact, cybersecurity, in a noteworthy change, has now made its way into the top five mission areas of the DHS, and I applaud that placement because that is exactly where I think it belongs.

The Bottom-Up Review is also a broad narrative of the Department's key missions—I will say for myself too broad at least in its first iteration and various of its parts—and its goals for improving those missions, which sometimes in the report seemed too vague to me as I read them. I hope, Ms. Lute, that you will be able to develop those in some more detail today and in follow-on documents.

When Congress created the Department of Homeland Security out of 22 different Federal agencies in 2002, we knew it would take time for it to mature into a cohesive agency that could focus its many parts on its two main missions, which are to take the lead in our Nation's fight against the Islamist terrorists who attacked us on September 11, 2001, and also to be able to respond better to natural disasters. I think overall, as I have said here many times before, the Department has done very well at achieving those missions, but it still has a way to go as we all acknowledge.

The QHSR and the BUR are important steps on the path to achieving that goal, and I have questions that I am going to ask about that.

I do want to say that we hold this hearing against the backdrop of a series of articles that has been in the *Washington Post* called "Top Secret America" that examines the new institutions and programs created after September 11, 2001, particularly focused on intelligence, but also including the Department of Homeland Security. So it makes this oversight of the QHSR and the BUR particularly timely.

I think the *Washington Post* series has raised important questions about the big changes in our government since September 11, 2001. For instance, is too much of our war against the terrorists who attacked us on September 11, 2001, being outsourced to private contractors? That is a big question raised by the *Washington Post* series; it is one that has been of concern to this Committee for some significant period of time, actually going back to October 2007, when we held a hearing on the Department's reliance on contractors. At that hearing, the Government Accountability Office (GAO) presented the results of a review that they conducted at the request of Senator Collins and myself. We have consistently pressed the Department on this issue in the context of our over-

sight of specific programs since then, such as SBInet and cyber functions, for example, where there continue to be a significant number of private contractors involved. The former Under Secretary for Management, Elaine Duke, I think, tried to dig into this issue toward the end of the last Administration but did not get very far, and I am not sure she had much support from people above her.

I am pleased to say that it does seem to me that a serious review of the contractor workforce is underway now under Secretary Janet Napolitano and Deputy Secretary Lute. At a briefing in December, we heard for the first time that DHS is trying to quantify the number of contract employees. The numbers that we have received are really quite remarkable. At an oversight hearing on this question a while ago, I was shocked to hear the number 200,000 contract employees that are working for the Department of Homeland Security, as compared to 188,000 full-time civilian employees.

After that hearing, Senator Collins and I wrote to Secretary Napolitano to ask for a more detailed breakdown on the contractor workforce so we could determine whether those contract employees were doing inherently governmental work in violation of the law. It is hard to imagine with so many that some of them were not, and I think we have to face that problem and deal with it so that the reality comes into conformance with the law.

While we have been assured repeatedly by the Department that a review is underway, we still, as of this morning, do not have a timetable for when that review will be complete or a specific breakdown at the program level of the current full-time employee to private contractor ratios.

I hope, Ms. Lute, that you will be able to help us answer some of these questions today, and if not today, then as soon as possible. In my opinion, a lot of the growth of the homeland security and intelligence community of the U.S. Government after September 11, 2001, was necessary, and I do not know if the series in the *Washington Post* intends to say that the system is out of control, but I do not find from my inquiry that it is out of control, both because of the creation of the Department, which is exercising management and coordination authority, and also in the intelligence area because of the creation of the Director of National Intelligence who is doing the same.

But there has been a lot of growth, and it has happened quickly. It is part of why we have been relatively fortunate since September 11, 2001, that, thank God, and thanks to all the employees of the government who have helped us do that, we have not been hit again with anything like September 11, 2001. But the facts in the *Washington Post* series, and all that we have been working on over the last 3 years here in the Committee, say that we cannot just let the machine operate without control from the Executive Branch and oversight from the Legislative Branch so that we are sure that we are spending taxpayer dollars in a cost-effective way.

I look forward to discussing this and all the other topics that the QHSR and the BUR raise with you this morning. I appreciate your being here.

Senator Collins.

# OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman. Thank you for holding this hearing on the need to establish clear priorities for the Department of Homeland Security, the Federal entity created to help protect our country from terrorism and other threats.

As has been stated many times, if you try to protect everything, you end up protecting nothing. So it is incumbent upon the Department, particularly when budgets are tight, to set detailed priorities to improve the preparedness and security of our Nation.

The Department's Quadrennial Homeland Security Review is a good first attempt to outline strategic homeland security missions and goals. Yet, the Department itself acknowledged that the QHSR was incomplete, so it then conducted a follow-on review. As the Chairman has indicated, this assessment, known as the Bottom-Up Review, was intended to set priorities for security initiatives and reorganization at the Department.

While I appreciate the Department's effort to undertake such a comprehensive analysis, the results are disappointing. Indeed, the two reviews simply do not compare to the level of analysis and planning that goes into the Quadrennial Defense Review and supporting documents. Let me give an example.

In the QDR and in the Navy's shipbuilding plan, the Department of Defense outlined specific measurable goals, such as a 313-ship Navy. The 30-year shipbuilding plan includes a force structure, construction plan, funding assumptions, and a specific articulation of the risk inherent in the force projections. By comparison, the Department of Homeland Security's reviews amount essentially to high-level strategy documents that provide little in the way of concrete goals or the actions needed to achieve them.

For example, the Department of Homeland Security reviews set some goals to eliminate unnecessary duplication, to decrease operational inefficiencies, and to promote cybersecurity. But without specific measurable plans, how can Congress hold the Department accountable for meeting these goals?

In these documents, the Department highlights the critical need to address the threat of a cyber attack and indeed lists cybersecurity as one of five strategic "pillars." I agree with that priority, but that seems inconsistent with the President's budget request for fiscal year 2011, which cut the Department's cybersecurity budget by \$19 million. How can the Department shoulder even the general responsibilities of an entire pillar while cutting the associated budget? The documents do not explain that contradiction, nor do they outline how the Department plans to do more with less.

As co-author with the Chairman of a comprehensive bipartisan cybersecurity bill, I am disappointed that the Department's reviews do not identify the authorities and resources that DHS will need to enhance its cybersecurity capabilities. The legislation this Committee approved last month would fill that gap.

The Bottom-Up Review also fails to provide any specificity, as the Chairman has indicated, on how the Department will reduce its troubling overreliance on contractors. This is a concern that I have raised repeatedly with the Secretary, as has the Chairman and other Committee members. As the *Washington Post* investigation revealed, six out of 10 employees at the DHS Office of Intelligence

and Analysis (I&A) are from private industry. This is on top of the revelation that an astonishing 50 percent of the DHS workforce are contractors. This is unacceptable.

Now, let me emphasize that I recognize that contractors play an important role in augmenting the Federal workforce in helping to meet a one-time need, but they cannot displace the need for permanent, well-trained government employees.

But what does the DHS report say about this? Simply that "DHS will continue to build on contractor conversion efforts at an even more aggressive pace." That is not a plan. It is simply a platitude.

Like a compass, the QHSR should aid the Department in aligning its budget requests with homeland security priorities, and in turn, these priorities would help Congress evaluate the President's budget request against measurable goals. The reviews that the Department has presented to Congress accomplish none of these tasks. They do not include a budget plan for the Department, nor do they assess how the organizational structure can better meet the national homeland security strategy.

I also have to mention an issue that the Chairman and I have mentioned repeatedly about documents presented to the public and our Committee. The QHSR slights the strategic threat posed by violent Islamist extremists by refusing to call that real and present danger what it is. This is ironic considering that the introduction to the QHSR discusses the Christmas Day attack, an attack conducted by a violent Islamist extremist. The review does not reference "violent Islamist extremism" or any variation of that phrase in the entirety of its 108 pages, and it refers to "homegrown extremists" only once. That is astonishing given the alarming increase in the number of homegrown terrorist plots last year. In sharp contrast, the October 2007 National Strategy for Homeland Security uses the word "Islamic" 15 times and the word "homegrown" eight times.

The Bottom-Up Review fails to describe how the Department will confront the threat of home-based terrorism. If DHS does not acknowledge in a forthright way the nature of the threat or explain how the Department intends to counter it, it is impossible for Congress and the American people to judge the Department's counter-terrorism plans and whether they are adequately reflected in its budget and priorities.

I look forward to hearing more from the Department's Deputy Secretary about how more concrete and actionable plans will be developed. That planning is essential to improve the efficiency of departmental operations and to build sensible budget plans. Only then will the time and effort—and I recognize there was tremendous time and effort put into these projects—spent on these reviews pay dividends in the form of a usable road map to better protect the American people.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you very much for that statement, Senator Collins.

Ms. Lute, again welcome. Thanks for all your good work for our country, and we look forward to your statement now.

**TESTIMONY OF HON. JANE HOLL LUTE,<sup>1</sup> DEPUTY SECRETARY,  
U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. LUTE. Thank you very much, Mr. Chairman, Ranking Member Collins, and Members of the Committee. I am happy to be here today to discuss the Department's Quadrennial Homeland Security Review and the Bottom-Up Review and, in particular, how the Department of Homeland Security plans to implement the initiatives set forth in these two efforts.

As you know, and as you have pointed out, the submission of the QHSR report to Congress earlier this year marked an important first step in a multi-step process to examine and address fundamental issues that concern the broadest perspective of what is called the homeland security enterprise.

The Bottom-Up Review was initiated in November 2009 as an immediate follow-up to complement the work of the QHSR with the aim to align the Department's programmatic activities and organizational structure with the broader strategic and mission direction identified in the QHSR. The BUR report itself reflects that endeavor and represents an intermediate step between the QHSR report and the President's fiscal year 2012 budget request and future years, which will propose specific programmatic adjustments based on the QHSR strategic framework.

The QHSR resulted in the articulation of a strategic framework and a positive, forward-looking vision for homeland security. Indeed, one of the initial challenges that we faced is that while homeland security had broad and widespread and extensive name recognition, brand recognition, there was less of a handle on what it meant to talk about a secure homeland. The QHSR lays out a vision for homeland security that says, very simply, we are trying to build a safe, secure, and resilient place against terrorism and other hazards where the American way of life, interests, and aspirations can thrive.

Informed by this conception of homeland security that is a positive, forward-looking vision, the report also places emphasis on the fact that it takes an enterprise, the homeland security enterprise, a more complete and comprehensive understanding of the homeland security threats, and the need to achieve balance across the efforts related to security, resilience, and the important elements of customs and exchange.

The QHSR strategic framework grounds homeland security, the achievement of this vision, in the accomplishment of five missions, and those missions are: Preventing terrorism and enhancing security; securing and managing our borders; enforcing and administering our immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. We believe that if we achieve these five missions and execute these five mission sets, we will go a long way toward achieving a safe, secure, and resilient place where the American way of life can thrive.

The Bottom-Up Review is the second major step of a three-part process that began with the QHSR. The BUR began with an activities inventory of all of the things the Department does on a daily basis. Of the 230,000 people that comprise the Federal workforce

<sup>1</sup>The prepared statement of Ms. Lute appears in the Appendix on page 33.

of the Department of Homeland Security, 225,000 of them are in the operating agencies. This is an operating Department. What do we do every day? And how do those activities every day contribute to the five missions we have identified as essential to building a safe, secure, and resilient place for the American way of life to thrive?

The BUR went beyond this taxonomy of the activities inventory and resulted in a clear sense of priorities across three main categories: One, how do we enhance our mission performance in the five areas I laid out? Two, how do we improve the way we run ourselves? And, three, how do we increase accountability for the resources that have been entrusted to us?

We have laid out a number of priorities in the Bottom-Up Review, and these are priorities that we believe should be implemented by the Department over the coming quadrennial. This is a 4-year list of priorities. We will not accomplish all 44 of the initiatives and enhancements in fiscal year 2012.

Several key themes emerged out of the QHSR and the Bottom-Up Review process. All of these are set forth in the Executive Summaries of the two reports, but I want to emphasize a few things that the QHSR and the BUR processes have brought forward.

First, an emphasis on the importance of the resilience of individuals and communities to our Nation's security.

Second, as the Ranking Member mentioned, the promotion of cybersecurity as a key homeland security mission.

Third, the recognition in a set of strategic documents that homeland security is a shared responsibility and that all of us—citizens, businesses, communities, Federal, State, local, territorial, and tribal governments, nongovernmental organizations, and the private sector—are part of the larger homeland security enterprise.

Fourth, the development through the Bottom-Up Review of a set of tools that will allow the Department for the first time to look at all of our activities across the five homeland security missions and assess their importance and contributions, not just from the perspective of the individual operating component, whether the Transportation Security Administration (TSA), the Federal Emergency Management Agency (FEMA), or the Coast Guard, but to each mission and to each specific set of critical functions. This will allow us to be better stewards of taxpayer dollars and to better manage the performance of our mission activities.

And, finally, that the initiatives and enhancements that have emerged from the QHSR and the Bottom-Up Review will materially benefit the citizens of this country and their communities.

It is unusual for a Federal department to have the opportunity to engage in the first principles that established it as a Federal agency and to engage in a comprehensive study of its missions from the bottom up and to evaluate each of its activities against priorities that have been identified from a thoroughgoing and broadly inclusive process. And DHS has benefited greatly from the experience.

Finally, Mr. Chairman, we have learned a few lessons in this process, and as we look forward to the next QHSR, I would like to share with you a few of those lessons.

First, senior leadership and engagement is critical. The support of Congress is equally critical as well, and the Department has benefited greatly from the support of this Committee and from other Members of Congress through this entire 18-month exercise that brought us to today.

Second, timing is important. The QHSR was conducted over a transition year. We lost valuable time in terms of consolidating the work that had been done in an effort to address all of the requirements that Congress laid out for us. This is why we took the approach we did to break it into three parts: The QHSR, the Bottom-Up Review, and the submission of the budget for fiscal year 2012.

Third, you must oblige yourself to take account of what has gone on before you. The Department of Homeland Security is 7 years old. I have said in many forums that this is good news. It is not 1 year old for the seventh time. There has been an enormous amount of work, thought, discipline, and activity that have gone on that we have been able to build on, expand on, and move on from this point forward.

In addition, the other major quadrennial reviews, including the QDR, and the first ever Quadrennial Diplomacy and Development Review, among others, must be synchronized, and the Administration made a concerted attempt to do just that. Today's security environment demands whole of government solutions and flexible and adaptable policy responses to difficult challenges.

Thank you again, Mr. Chairman, for the opportunity to come speak with you today about implementation of the QHSR and Bottom-Up Review and the lessons learned for the future. I have submitted my full testimony for the record and look forward to the questions of the Committee.

Chairman LIEBERMAN. Thanks very much, Ms. Lute, for that opening statement. Let me say we will do 7-minute rounds of questions. Senator Collins left, but she will be back. She has an Appropriations Subcommittee meeting that she has to attend.

Let me begin with the question, which is somewhat off the QHSR, but not really—which is about the private contractor workforce in DHS. I will give an example of some specific areas for concern.

In the office overseeing the National Cybersecurity Protection System, there are 122 contract support staff but only 11 government employees. The latest numbers for the Intelligence and Analysis Section of the Department show that about 53 percent of its workers are contractors.

In the Department's fiscal year 2011 budget submission, there were identified approximately 3,300 contractor positions that would be converted to Federal employees. Of course, at that rate it is going to be a long time, a lot of decades before we get the number of private contract employees down.

In May, our Subcommittee headed by Senator Akaka and Senator Voinovich held a hearing, and the Chief Human Capital Officer reported on the broader process that the Department is undertaking through its Balanced Workforce Initiative to achieve the appropriate balance between full-time Federal employees and contractors. The BUR again notes that the Department will continue to



build on these efforts, although no details on the review are provided.

So let me ask you to address yourself to this question. The first really is process. When will we see the specifics of the Department's review of its private contractor workforce in relationship to the full-time Federal employees?

Ms. LUTE. Thank you, Mr. Chairman. We are working intensively on this issue. As you know, certainly, and Members of this Committee know well, the Department was stood up in part with an explicit reliance on a contract workforce to be able to get the Department up and running, and we continue to rely on hard-working contractors who come to work believing in the mission and the purpose of homeland security every day.

The Balanced Workforce Initiative—and I just issued a series of instructions earlier this month to the leadership of the operating components regarding their personal association with the Balanced Workforce Initiative—is designed to give us a handle on strategic workforce planning. In order to do that, Mr. Chairman, what we also did as part of the Bottom-Up Review process was begin a procedure to allow us to align our accounting properly so that we could tell personnel costs across the operating component because they were all counted differently. So before we could run, we needed to walk; and before we could walk, we needed to crawl. And we are doing these things somewhat simultaneously. So we are getting a handle exactly on where our workforce and personnel are assigned, how they are assigned to the critical missions that are the sub-components of each of the missions outlined in the QHSR, and then we are moving through systematically on a priority basis to see where contractors are present and work aggressively to convert them.

Chairman LIEBERMAN. Do you have a timeline, a goal by which you hope to finish this review and report to us?

Ms. LUTE. Yes, we certainly hope to finish it this year, Mr. Chairman, and map our way forward.

Chairman LIEBERMAN. So you are saying this calendar year. I guess the question is whether as a result you may be able to undertake a significant realignment of the workforce for the fiscal year 2012 budget.

Ms. LUTE. We certainly hope to do that, Mr. Chairman.

Chairman LIEBERMAN. Let me ask you just for a quick response because you had a lot of experience in governmental administration. There is nothing inherently wrong with a private contractor being retained by a government agency. It has happened probably since the beginning of our government. But I wonder if you would talk a little bit about the balance there.

For instance, on average, what is your sense of whether it costs us more, taking all the costs in mind and account, for a private contract employee or for a full-time Federal employee?

Ms. LUTE. It depends on the circumstances, Mr. Chairman. If it is for a short-term requirement, it may be more cost efficient to have contractors. For longer-term steady state need—

Chairman LIEBERMAN. More efficient because you are not building in the long-term commitment that comes with retaining a full-time employee.

Ms. LUTE. Exactly.

Chairman LIEBERMAN. Yes. I hope that will be part of your review. You are right that we expected in standing up the Department that, particularly in getting into areas that we had not been in before, like cybersecurity, there would be a lot of contract employees hired. But certainly the numbers are stunning, the number of contract employees larger overall than the number of full-time Federal employees. And I think this cries out for just what you have said in the title of the review, which is to balance the workforce consistent with the law.

Let me leave that there and go on to a question about intelligence and analysis.

The *Washington Post* series—I will lead into it with this—talks about a growth in not just contractors but people involved in intelligence. And, of course, in creating the Department of Homeland Security, we created an entire new intelligence operation, which we hoped would have a kind of value-added to it, a unique aspect to it. And, again, I know that a lot of the employees of I&A at the Department of Homeland Security are contract employees. So I want to ask you two questions.

First, if somebody reading the *Washington Post* series asked if you are just duplicating in this intelligence department at the Department of Homeland Security what exists elsewhere, what would you say?

And second, I trust that you are trying to bring on more full-time Federal employees in the intelligence section of the Department of Homeland Security so that this imbalance of more contractors than full-time workers will be eliminated.

Ms. LUTE. Well, thanks, Mr. Chairman. First what I would say is no, we are not duplicating it. One of the things that we have been able to do over the past year and a half is really drill into what the value proposition of the headquarters of the Department of Homeland Security is, and I&A is a vital part of that.

The value proposition of I&A is to equip the entire homeland security enterprise with the information and intelligence it needs to discharge all of the homeland security missions. There is no other part of the intelligence community that is oriented on that challenge, and I&A performs that function critically in support of all of the operating components. So that is what I would say primarily.

Chairman LIEBERMAN. So you would say that I&A in DHS is drawing from the rest of the intelligence community information that it is producing, but I&A is producing its own information that is also being shared with the rest of the community.

Ms. LUTE. Yes.

Chairman LIEBERMAN. One of our hopes when we created the Department was that a lot of the intelligence work that is naturally done by components of DHS, including the Coast Guard or the kind of information that Customs and Border Protection (CBP) comes up with, would be fed more routinely into the pool of intelligence from which everybody can draw, and also, of course, that DHS would play a unique role here in drawing intelligence from State and local law enforcement officials and also returning intelligence in accessible packages to them. Is that latter function being carried out by I&A at this point?

Ms. LUTE. It is, Mr. Chairman, and, in fact, this is an area where we really want to emphasize in building up the fusion centers that exist precisely for that purpose.

I would back up and say, Mr. Chairman, with respect to the issue of terrorism and combatting terrorism and the potential for a terrorist strike in this country, the Department of Homeland Security has, through its border agencies and other agencies, daily interaction with the global movement of people and goods and substantial amounts of information regarding that movement in order for us to properly identify dangers where they exist and expedite legitimate trade and travel, which must go on. And we certainly are vibrant and active members of the entire whole of government approach in that regard.

And, finally, Mr. Chairman, if I might, a word on the numbers with respect to I&A. Not surprisingly, you will hear me say that the *Washington Post* is wrong in saying that—

Chairman LIEBERMAN. You are not going to be punished in this room for saying that. [Laughter.]

Ms. LUTE. And, in fact, if all of our full-time Federal employees were on hand in I&A, the number would be closer to four out of 10 rather than six out of 10, and so this is an issue we are working on.

Chairman LIEBERMAN. Good. I appreciate it. You made a very important point at the end, which I just want to put an exclamation point next to. I know that the Committee knows that, for instance, in the really remarkable work done to apprehend Najibullah Zazi and David Coleman Headley before they were able to carry out terrorist acts, the intelligence sections, particularly the databases that Customs and Border Protection has, for instance, were critically important in apprehending those two. And, of course, it was CBP that stopped ultimately Faisal Shahzad before he left America on that plane after attempting to blow up the bomb in Times Square. So I thank you for that.

Senator Voinovich.

#### OPENING STATEMENT OF SENATOR VOINOVICH

Senator VOINOVICH. Thank you, Mr. Chairman.

First of all, before I get into some of my comments and questions, I have been trying since February, again in March, and as recently as last week, to get an answer from the Department on whether or not the Biometric Air Exit Program should be decoupled from further expansion of the Visa Waiver Program. I am very frustrated about that kind of turnaround on a response to a Member of the U.S. Senate. I am the sponsor of the legislation on the visa waiver program. I have asked for that response time and time again, and I cannot get it, and I am very upset about it. And I am telling you about it, and you should tell the Secretary that I am about ready to go to the floor to talk about the incompetence of your Department in not being able to get back to a Member of Congress with a simple answer to a question, and you have had plenty of time to look at it.

Second of all, this Department has been on the high-risk list since 2003—22 agencies, 210,000 employees, 225 contractors, 45-

percent increase in the budget—and I have not heard anything about more with less or we are working harder and smarter.

We have a very difficult budgetary environment right now. I happen to be the Ranking Member on the Appropriations Subcommittee on Homeland Security, and we are trying to get the overall spending level down. And it appears to me that what may have been the Federal role in the aftermath of September 11, 2001, seems increasingly less appropriate when you give considerations to some of the things that we are doing in the Department.

The Committee has learned time and time again that FEMA does not employ performance metrics that adequately assess the results of grant program funding. The few metrics that do exist are output-based rather than outcome-based. As my colleagues know, measuring a program's outputs provides little insight into its effectiveness.

FEMA also persistently fails to allocate State Homeland Security Program and Urban Area Security Initiative funding according to risk. A June 2008 Government Accountability Office report found that when determining grant allocations, FEMA assigns the same vulnerability rating to all localities regardless of their unique features. And that arrangement remains in place today.

One of the things that I remember clearly when the 9/11 Commission came back with their recommendations, they said homeland security assistance should be based strictly on assessments of risks and vulnerability, and not according to a general revenue-sharing arrangement like the kind that exists today. And I know that when September 11, 2001, occurred, I said we are going to have to spend more money, but we have to be careful—and I said this as a former governor and mayor—that it not turn into a revenue-sharing program.

So I am looking at your budget now to figure out some ways, maybe, that we can reduce some of the funding that is in that budget.

For example, we have the firefighter grants. We still have \$150 million in unobligated funds from the 2009 budget. We have not spent a dime of the \$810 million in this fiscal year's budget. It would seem to me that in light of that we could just say put nothing in the 2011 budget when you have over \$1 billion hanging out there that nobody has even made application for.

The Urban Area Security Initiative grants—at one time, in 2003, we had 29. Today we have 64 of them. And instead of sending money to every city in America, we should restrict funding to the top cities that face the threats. We are in a tight budgetary situation today, and the Department ought to be looking at these programs and saying are these really relevant to securing the homeland.

Our homeland security grants—today we spend \$950 million on those, and the program gets funded year after year without anyone having an idea if these dollars are being used effectively to reduce risk in this country.

So we have this whole business of evaluating and looking at risks and where is the money going to. When are you going to start to look at these things? One of the things that I thought the Department did several years ago is that you did an assessment of inter-

operability in the various States. That was terrific for me because I read the report, I went out to the four areas in Ohio, went to the cities, visited with them, spent a day asking what are you doing with interoperability, how is it working and so forth. You just cannot keep going the way you are going. And what are you going to do to start looking at some of this stuff? You are going to have a tighter budget, and it is going to get worse as time goes on. What are you going to do about this?

Ms. LUTE. Thanks, Senator. A couple of things.

We recognize that we are in different budgetary times than the Department has experienced since its founding. Congress has been very generous to the Department of Homeland Security and expectations have grown equally. The mandate and responsibilities given to the Department are extraordinary, as this Committee well knows. But we must get a tighter rein on our spending, and we have tried to do that through the BUR process and doing what I have been calling the plumbing and wiring of institution strengthening so that we can be responsible stewards for the resources that have been given to us and that we can manage ourselves more effectively.

Part of the BUR process has included, as I mentioned, an activities inventory. What are we doing every day and do those activities match to the missions, to the goals, and to the objectives that we say are most important? If they are not, we should really stop doing them or look at alternative ways to achieve what they were designed to do in support of those missions, goals, and objectives.

Second, we are trying to align our account structure so that we can compare personnel across the Department, which we currently cannot do, so that we can compare investments across the Department, operating and maintenance costs across the Department, and understand the value proposition of applying in a border region, for example, the resources of CBP, TSA, Immigration and Customs Enforcement (ICE), and the Coast Guard appropriately, and do that in a way that is rationalized, as you mentioned, to risk.

But I want to spend a moment on performance measures because the performance measures that we have been operating with in the Department do not reveal to the American public, or surely to this body or even to ourselves, the kinds of things that we need to see to know that, in fact, the United States is becoming more secure, that we are achieving our mission sets.

Senator VOINOVICH. Let me just say this, as a simple matter. Some of this stuff is not real complicated, and I am familiar with what you have done on the border. I have had some problems with your buying airport screening machinery with body imaging capabilities. I have been briefed. You have done a good job of convincing me that it is needed. There are other things that are needed in the Department, but do you need to put another almost \$800 million into the firefighter grants when you have not spent \$150 million of the 2009 and 2010 money? There is an area, it seems to me, that could be looked at, where you could say to our Committee that you do not need this money right now. If you did not get this money, you could reduce your overall cost. You could, for example, replace a helicopter that you are going to need because one went down out in California. The urban security grants, giving all this money out

all over the country to people—for what reason? Why are we doing it? What are you getting out of it?

It just seems to me that you have an obligation to start looking at these programs and coming back to Congress and saying this is not needed right now. Even some of the areas that got a whole bunch of money in the beginning, they did the infrastructure, they put in the cameras, they put in all of the stuff that is necessary, and yet they are still getting about the same or even more money than they were getting before they made these capital expenditures.

Now, I understand if they want to argue and say we need that money so that we can hire more people to do something that we would not ordinarily do, but we have to have some rationale about this. And your people ought to be getting at it.

Ms. LUTE. We agree, Senator. We are looking at all of our risk frameworks and approaches across the entire Department, not only in the context of the challenges and threats that we currently face, but also in the context of the investments and expenditures that have gone on before. We are very mindful of this, and we are also very mindful that as we outlined in the QHSR—

Senator VOINOVICH. Let me say this to you: It was not reflected in the budget that you submitted to the U.S. Senate this year.

Ms. LUTE. What I can say to you, Senator, is that, as we have said in the QHSR, the security of the American homeland takes an enterprise. It takes informed individuals, it takes capable communities, and it takes a responsive Federal system all working together to achieve a secure homeland, and we recognize that the Department plays a key role in leading the Federal effort in this regard together with State and local officials.

We are looking at all of our expenditures in the current fiscal climate and assessing all of our risk frameworks, and we believe we can and will do better.

Chairman LIEBERMAN. Thanks, Senator Voinovich.

Secretary Lute, I do not think I heard you respond to Senator Voinovich's concern about a lack of a response to his questions about the Visa Waiver Program.

Ms. LUTE. I apologize, Senator. Inordinate delay is unacceptable. I will not offer an excuse. I believe the Secretary signed earlier this week a response to you.

Senator VOINOVICH. We have talked about this.

Chairman LIEBERMAN. Yes, for sure.

Senator VOINOVICH. You helped draft the legislation, and they put no money in the budget to pay for establishing a biometric air exit program.

Chairman LIEBERMAN. Right.

Senator VOINOVICH. And I said, well, if you do not think it is necessary—and they said they do not think it is necessary—then you ought to get back to us and say that we do not think it is necessary, that we are tracking this in some other fashion, and allow us to get rid of that provision and go back to the 10 percent rather than the 3 percent today.

Chairman LIEBERMAN. Yes, this is really important.

Senator Voinovich speaks for the whole Committee on this, so I look forward to seeing what the Secretary's response is because as

he said, we required that the biometric be in place before we allowed anyone to come into the program if they were over that 3 percent, and we actually put a waiver of 10 percent into the law, but we have suspended that pending the coming of the biometric. So that is a very important letter to have answered. Thanks for raising it, Senator Voinovich, and thanks for your response, Ms. Lute. And so please do everything you can to make sure that letter gets to Senator Voinovich quickly.

Senator Brown, welcome.

#### **OPENING STATEMENT OF SENATOR BROWN**

Senator BROWN. Thank you, Mr. Chairman. It is good to be here. I am going to have a few questions, and I will submit a couple for the record because I have a couple of other hearings. I am bouncing back and forth, too, so thank you.

What do you think DHS has learned from this review that will translate to 2013? Are there any lessons that you can share with us?

Ms. LUTE. Leaders have to be engaged. This is a leadership exercise, and it has to be led from the top.

Second, the timing of the review is important. Transition years are difficult to manage efforts like this if you are looking for as comprehensive an analysis of the homeland security enterprise as you are.

The third lesson that I have learned is kind of a personal lesson, I suppose. Homeland security is very different from national security where I have spent my whole career. National security is centralized, strategic, and top-driven. Homeland security is decentralized; it is operational, and it is drive from the grass roots up. It is an enterprise that involves every American, every community, every State, territory, and tribal entity as well. So we need to have an inclusive process and opportunities for voices to be heard on these critical issues. We tried to do that in the QHSR. I would urge that this lesson be replicated the next time this occurs.

Fourth, you must learn from what has gone on before you. Do not make the mistake of thinking that you are discovering things. Learn to distinguish what is new from what is new to you. Build on the work that has gone on thus far. Look at where the investments have been made. Understand the rationales. Build out the capabilities. Be explicit in understanding what it will take to achieve the missions that you say are so central to the vision you are trying to create. In our case, we articulate a safe, secure, and resilient place where the American way of life can thrive. We think it takes five missions: Preventing terrorism, securing our borders, enforcing our immigration laws, ensuring our cybersecurity, and ensuring resilience of the American society against all hazards.

How will we know if we have achieved those objectives? The QHSR lays that pathway out. And have nerves of steel because there will be people who will challenge you and question you. It is their right to do so, and the outcome will be the better and richer for it if you face the big league pitching of the best ideas that are out there.

Senator BROWN. Thank you for that response. You talked about leadership and grass roots. Well, I think leadership starts from the

top. I know I am new here, but taking so long to respond to Senator Voinovich's and Senator Lieberman's pretty simple request is really unheard of. And the thing that I am noticing is that there is a disconnect sometimes between the Senate and the Administration by not addressing very basic concerns because we are not making this stuff up. We usually get questions from our constituents who put us in office, who ultimately put people in the Administration in office, and we need to have the answers to a lot of these questions. And we do not need them in months. We need them usually in a day or two.

And so I would encourage you and every other department in the Federal Government to get with it and start getting us the answers we need so we can respond properly.

I also, as you may or may not know, am the Ranking Member on the Contracting Oversight Subcommittee, and we have had a lot of hearings, and I tell you that Senator Voinovich was right on the money. You have not used money, yet you are asking for more money. And we are using contractors, and we are giving them bonuses when they mess up and when they are in default, or they owe us money that they have owed us for years. So I do not if it is a question or a comment, but I would encourage you, because we are at \$13 trillion and counting, if there is any streamlining, consolidation, or eliminating of overlap that you can do in your Department to save the taxpayers some good funds, that would be greatly appreciated.

Ms. LUTE. Senator, I would just say that I absolutely agree with that. I certainly agree with that. One of the initiatives that we are pursuing in the Department, and have been and now are reaching a point where we will greatly accelerate our work, is looking at our whole acquisition process. Can we improve our ability to set requirements in reliable ways that allow effective contract mechanisms? Do we have the kind of program management and oversight for those contracts as well, again, building on work that has been done previously.

So what I can tell you is that through efficiency reviews that the Secretary has ordered over the past 18 months, we have saved over \$100 million, and we look forward to sharing those details shortly.

Senator BROWN. Well, the comment, can you do this, yes, you can do it. You can do these things. Every agency can do these things. I tell you, the rhetoric—we have saved \$100 million here—with all due respect, \$100 million in Washington is nothing. We are talking billions here. I would like to see some real savings. And can you do it? Yes, you should do it, and so should every other agency make it their No. 1 priority to start saving taxpayer dollars and putting them where it is effective.

And with regard to closing borders, yes, you should jump on Arizona and get that squared away right away because until the borders are secure in our country, how do we address all the other issues that flow down from that?

I thank you, Mr. Chairman. I have other questions, but I have to get to the other hearing.

Chairman LIEBERMAN. Thanks, Senator Brown, very much for coming by and for asking those questions, and we will enter your other questions in the record.



We will go to a second round of questions now.

Ms. Lute, I know you have explained that the Bottom-Up Review includes 44 initiatives and enhancements that have been recognized by the Department as priorities for the next 4 years. I understand, of course, that not every worthwhile project can be included in the list of priorities, but there are a couple that are omitted that are troublesome to me, and the one that I particularly want to ask about is rail and transit security because the fact is it seems to me that the Secretary and now John Pistole coming in at TSA have pledged to give more attention than has been the case in the past to rail and transit security. So I want to ask you why rail and transit security was not highlighted by either the QHSR or the BUR and what DHS plans to do to address those non-aviation forms of transportation, which, of course, in other countries have been attacked by terrorists and in our country in the case of Zazi were intended targets for attack?

Ms. LUTE. Mr. Chairman, we think we do identify mass transit, rail, and other transportation infrastructure as key, obviously, to the security of this country. We also highlight the vulnerability of these systems, recognizing that many of the systems exist in private sector hands. We highlight our awareness of the vulnerabilities of these systems to terrorist attacks. We have been and we will continue to work with the private sector in a concerted effort and also with the American public. The launching of the nationwide campaign built on the New York model of "See something, say something" is precisely designed to enlist the extraordinary capacity of the American public as well. And so we do believe that transportation security involves far more than aviation. Aviation is a priority. It will be something that we are stressing. The Secretary has been working, as you well know, through the beginning of this year on a stronger international aviation security regime because we know that if you have access to any part of the system, you potentially have access to the entire system, and we need to work on that as a priority matter.

Chairman LIEBERMAN. I appreciate that. So I take from your statement that rail and transit security, notwithstanding the particulars of those 44, remains a priority for the Department.

Ms. LUTE. Absolutely.

Chairman LIEBERMAN. Let me ask you about a couple of the structural changes that are called for in the Bottom-Up Review, which I found interesting. The first is the call for a "single coordinating entity" across the Department for counterterrorism activities. I know that in March of this year, Secretary Napolitano designated the Under Secretary for the National Protection and Programs Directorate, Rand Beers, as the DHS Coordinator for Counterterrorism.

I wanted to ask you just to talk a little bit about why the BUR and you conclude that this is necessary and how you think it will help the Department achieve its mission of protecting our homeland security.

Ms. LUTE. Thanks, Mr. Chairman. What we are trying to achieve in our preventing terrorism and counterterrorism agenda is an ability to leverage all parts of the Department as relevant for ad-

addressing the terrorism threat and also to leverage in turn a whole of government approach where necessary to do so.

It is very clear to us that beneath the level of the Secretary and myself, there does need to be a coming together and an ability to coordinate the various activities—CBP, TSA, etc. This is something that the Secretary takes very seriously, I take very seriously, and an enormous amount of our time is spent on ensuring that this country is protected against another terrorist attack.

We believe also that we need to look in a very deliberate way at the tools that are available to us to prevent terrorism here domestically. We have our border tools. These are key and essential, as I mentioned earlier. We have law enforcement tools, not only the law enforcement resources that exist in our Department and the FBI and other parts of the Federal system, but also, importantly, the 800,000 State and local law enforcement entities as well. We have intelligence and information sharing, as we previously discussed, and we have the American public.

So pulling all of these things together is something that we are working on. The designation of a coordinator is an interim solution pending a final review of how best to organize the Department to achieve these synergies.

Chairman LIEBERMAN. Good. Keep us posted on your work on that.

The other proposal that I wanted to talk about, which I think makes sense and yet I also think will have some problems in being implemented, is the idea of realigning the various regional configurations within the components of the Department of Homeland Security into a single Department of Homeland Security regional structure. So what are we talking about? DHS units have seven different regional structures. The Coast Guard may have one, CBP may have another, and FEMA may have another.

Obviously, one of the challenges in creating a single regional system for the Department is that the components' distinct organizations may in some cases have developed particular organizational needs. For instance, the Coast Guard's districts are typically focused on the coastal United States with a single large district covering much of the inland United States, while Customs and Border Protection's regions obviously reflect the importance of the border.

In carrying out this recommendation, how are you going to balance these two public interests?

Ms. LUTE. You are absolutely right, Mr. Chairman. On the one hand, the existence of seven separate, different regional structures in addressing homeland security issues in the United States seems excessive. On the other hand, we do not believe in a simple one size fits all approach, unmindful of the particular needs, and you mentioned the two components that are the most geographically fixed.

Chairman LIEBERMAN. Right.

Ms. LUTE. So as we proceed forward, we would look to work closely with this Committee and other Members of Congress to achieve the kind of regional structure and approach that allows us to achieve the integration of homeland security efforts and mission accomplishment, mindful of the realities on the ground.

Chairman LIEBERMAN. So it is probably going to be hard to have a single departmental regional structure.

Ms. LUTE. It may be hard——

Chairman LIEBERMAN. Although you can certainly have less than seven.

Ms. LUTE. But we think certainly it is something that we need to look at.

Chairman LIEBERMAN. I appreciate that. Thank you. My time is up.

Senator Collins, welcome back from the Appropriations Subcommittee meeting.

Senator COLLINS. Thank you, Mr. Chairman, and thank you for explaining my absence as well.

Ms. Lute, let me start where the Chairman just left off. I do believe that there are efficiencies and cost savings that can be achieved by consolidating some of the regional offices of DHS. But the Chairman's point about the Coast Guard is a very important one.

Obviously, there are some regional offices where the Coast Guard's role is minimal, but on the coasts of this country, the Coast Guard is absolutely essential, and trying to shoehorn the Coast Guard into a broader DHS office may end up costing money and decreasing the effectiveness of the Coast Guard.

Another agency, however, that you also need to take a close look at what you are doing in that area is FEMA. One of the lessons of the extensive investigation we did into the failed response to Hurricane Katrina was that there needed to be a regional FEMA presence that worked collaboratively all year round with its State, local, and other Federal partners and with the private sector, exercising together, planning together. As we found out during Hurricane Katrina, in the midst of a disaster is no time for people to be meeting each other for the first time, and yet that is exactly what we found. And that is why, as part of our FEMA reform bill, we specifically established FEMA regional offices.

How do you see FEMA fitting into your consolidation of regional offices?

Ms. LUTE. Thanks, Senator. Craig Fugate and I have talked a lot about this because I could not agree with you more. When I was in the Army, we used to say that you fight like you train, and that is certainly true for crisis response. A crisis is no time to put together an ad hoc organization in haste. Relationships matter and an understanding of capabilities matters and an understanding of the geography, the access, the particular needs of a community matters, and regions will not substitute for the State and local knowledge that exists, but these regions have to be important complements and points of synergy and leverage, as this Committee knows very well.

I have asked CBP and Coast Guard to begin the process of looking at whether and how we could consolidate some of our regional structures together with FEMA. Obviously, this bears on all of the operating components, as well, because they all have regional structures. But we do believe that we can consolidate some of the literally thousands of facilities that DHS has across the country.

Senator COLLINS. I think that is absolutely the case, and you can save money and actually enhance efficiency if the agencies are co-located in many cases. But I would caution you against assuming

that what works in Arizona for a regional office will work in New England. The needs and the roles of the various DHS agencies are extremely different depending on what region you are talking about.

One of my frustrations with the Department and, frankly, with the Bottom-Up Review is that there are longstanding problems, which precede this Administration, that the Department still is not tackling and solving. And I want to give you two examples.

At a hearing that our Committee held last month, the GAO testified that the Department still lacks a strategic plan for the screening of illicit nuclear and radiological materials that could come across our borders. The GAO first identified this necessity more than 7 years ago.

Now, the QHSR does state that one of the Department's goals is to "prevent the unauthorized acquisition or use" of nuclear and radiological materials along with biological and chemical weapons. But the Bottom-Up Review does not provide the kind of strategic direction that GAO identified 7 years ago and that our Committee has repeatedly pushed. And the lack of that plan has directly caused DHS to waste money, hundreds of millions of dollars, and to go off in one direction 1 year and another direction the other year.

It disappoints me that rather than completing this plan, the Bottom-Up Review just states that DHS will "leverage the full range of capabilities" and "increase its leadership role."

Those are just buzz words. They do not substitute for the kind of plan for which the GAO has been calling for 7 years.

When will DHS complete that important strategic plan? It is hard to think of something more pressing than making sure that radiological, nuclear, chemical, and biological weapons are not smuggled into this country.

Ms. LUTE. Senator, I agree with you. The BUR does identify as an initiative that we will increase efforts to detect and counter these dangerous weapons and dangerous materials, but how we will do that is the heart of your question.

I have just convened a series of meetings on exactly this issue. I will chair a working group within the Department to generate a concrete plan for us to present—and we look forward to working closely with this Committee on that plan—on how the Department can play its role in reducing the risk of nuclear terrorism, the terrorism associated with these most dangerous weapons.

In order to do that, we know that we must anticipate threats and protect against hostile use. In order to do that, we know we must ask: Who are the individuals seeking to acquire this? Where does this material exist? What are the lines of communications? What are the methods by which these individuals would seek to bring this material into this country? And what are the right strategies, leveraging, again, all of the resources that exist in the United States to protect against that?

Senator COLLINS. So when will the plan be completed?

Ms. LUTE. We are in the process of working on it, Senator. I cannot give you a precise month, but I will go back and as a matter of urgency set a timeline and be in touch with you.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks very much, Senator Collins.  
 Senator McCain, good morning.

#### OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Good morning, Mr. Chairman.

I was just looking at Appendix 1, the list of Bottom-Up Review initiatives and enhancements, and I must say that it is a wonderful and impressive list.

For example, I guess, one is enhance the DHS workforce. That is a good idea. Increase analytic capability and capacity. That is a good idea. There are really a lot of great ideas here, I would say to the witness, and I would love to see some actual accomplishments that have been achieved over the last 7 years or the last year and a half of this Administration as to how "enhance the DHS workforce" has taken place.

And I was struck by, for example, number 17, comprehensive immigration reform. Now, maybe you could fill me in on what your agency is going to do as its initiative or enhancement of comprehensive immigration reform.

Ms. LUTE. Senator, as you know, the President has made clear his desire to pursue comprehensive immigration reform. The Secretary has talked about it equally. The enhancements that we talk about—

Senator MCCAIN. So is that an initiative or an enhancement?

Ms. LUTE. The comprehensive immigration reform is an initiative of the Administration. If I were to talk about the enhancement of the—

Senator MCCAIN. I thought this was not an Administration initiative. I thought this was a Bottom-Up Review of the homeland security initiatives and enhancements. So you are just saying that is an overall Administration goal, so, therefore, it is your goal. Is that what you are saying?

Ms. LUTE. The Department discharges the responsibility for administering and enforcing the immigration laws of this country, Senator, as you well know, and this is an important feature of the way going forward—

Senator MCCAIN. That is your job, to enact comprehensive immigration reform? That is your initiative?

Ms. LUTE. No. I apologize if I misspoke. What I said is we have the responsibility to administer—

Senator MCCAIN. To administer.

Ms. LUTE [continuing]. And enforce the immigration laws.

Senator MCCAIN. But not take the initiative.

Look, the point is that this list here is really entertaining. Strengthen aviation security, create an integrated departmental information-sharing architecture. I would like to know what has been done in the last 7 years of these lists of initiatives and enhancements. Dismantle human smuggling organizations. There is nothing in this that anyone could argue with except that we would like to see some results. Apparently, the size of your organization continues to grow, and there seems to be arguments that our border is "as secure as it ever was" while the terrorism and violence on the other side of the border continues to grow, the latest being the

car bombing in Juarez. And so these are enhancements and initiatives.

What I would like to see, Mr. Chairman, is what the Homeland Security Department has done to carry out these motherhood-and-apple-pie initiatives and enhancements. And for you to come before this Committee and say that this is a list of initiatives and enhancements, I think, is laughable. And I would hope that maybe we would, as a Committee, demand that we know what the actual results are of these motherhood-and-apple-pie initiatives.

If I were you, I would be a little embarrassed to come before this Committee with this kind of a list of initiatives and enhancements, which are, at least according to your testimony so far, that we all agree that we ought to do better. I have not heard yet a single concrete example of what you have done to make these initiatives and enhancements a reality. And maybe you could supply those for the record.

Ms. LUTE. I would be happy to, Senator.

Chairman LIEBERMAN. Senator McCain, as you can hear from statements that I made earlier, and Senator Collins did, too, the BUR statements are general, they are vague. Let me ask you because it is my understanding, both from what you have implied here today and what the Department has said to our staff, that there are implementing directives to all 44 of these that are being circulated in the Department. Is that right?

Ms. LUTE. We are working on all of these initiatives, Senator, to give a concrete path forward on them, some of which, as I mentioned earlier, we will prioritize for the 2012 budget submission when the President presents that. These are initiatives that we believe over the quadrennial speak to areas that would be high-priority areas of focus for us in strengthening our ability to execute the mission sets that we have outlined in the QHSR, which we think are central to achieving the vision that we have outlined.

Chairman LIEBERMAN. There is nothing classified about those implementation plans. So as you get them together, I think it really would be helpful to the Committee if you would send us copies of them because the state of the document now is unsatisfying because it is unclear because of its lack of detail.

Senator MCCAIN. Mr. Chairman, could I also suggest that maybe the Department of Homeland Security should look at what the Department of Defense does on the Quadrennial Defense Review where there are specifics as to what initiatives need to be taken, what action has been taken, and what needs to be done. I have been around here a long time. This is one of the more remarkable things that I have ever seen, and, frankly, it is kind of disrespectful to the jurisdiction of this Committee to hand us a paper like this and expect that to be in any way helpful to us in our oversight responsibilities of what is now growing to be one of the largest agencies of government.

Chairman LIEBERMAN. The idea of the comparison to the QDR is an important one. Actually, Senator Collins mentioned it in her opening statement, and I would urge you to take a look at that and respond.

Senator Collins, you missed a round, so I want to give you the opportunity to ask some more questions at this point.

Senator COLLINS. Thank you so much, Mr. Chairman. Most of them I will submit for the record so that I am not holding everyone up, but there are a few that I do want to pursue.

Ms. Lute, I mentioned my disappointment at the lack of a specific plan for dealing with the nuclear and radiological weapons smuggling. But I want to give you another example of an area that this Committee identified first in June 2008, again in 2009, and again, the two reports you have provided do not have any specifics for correcting the problems. It is very frustrating that over and over this Committee has brought to the Department's attention severe shortcomings, and yet there is no sense of urgency on the part of the Department.

In this case, it has to do with the Federal Protective Service, and what we found is that GAO did a series of covert tests that revealed serious security vulnerabilities of Federal buildings with explosive devices easily being smuggled into 10 Federal buildings. And it is now 2010, 2 years later from when these problems were first brought to the Department's attention, and yet all that DHS says in the BUR report is that it "now proposes to undertake a major redesign of the Federal Protective Service."

It is extremely frustrating to me to have a serious problem brought to the attention of the Department 2 years ago and all that is in the BUR is a statement saying that the Department now proposes to undertake a redesign. Why are we not further along?

Ms. LUTE. Senator, I hear your frustration on the issue of why we are not further along. I can assure you that the Secretary and I and the leadership of the Department come to work every day with a sense of urgency about all of the missions that we have in homeland security. The Federal Protective Service, as you know, was just placed into the National Protection and Programs Directorate (NPPD), and as a consequence of that movement, of these reports that have come to light, and of our sense of the importance of the mission, the organization, the nature of the workforce, the training, etc., we have an obligation to present a comprehensive plan to bring the Federal Protective Service to the level of performance that everyone has a right to expect.

Senator COLLINS. Well, again, I want to see specific action in that area as well.

Let me switch to cybersecurity, an issue that I think is of great priority, and I was pleased to see that it is identified as one of the five primary missions of DHS by your review.

Do you agree that the Department needs new authorities and resources to perform its cybersecurity mission?

Ms. LUTE. We do think that the Department's ability to discharge its cybersecurity mission would be enhanced by those, yes.

Senator COLLINS. The Department's budget request for the cybersecurity division for fiscal year 2011 is \$19 million less than it was funded for this fiscal year. Do you anticipate that the Department will request additional funding for cybersecurity for the fiscal year 2012 budget so that you can fulfill this mandate?

Ms. LUTE. Without giving you a specific answer, Senator, we could. What we want to look at in our cybersecurity mission is precisely how do we fill out the space that we have been given with respect to responsibilities for securing the dot-gov and extending

into the dot-com domain as well. How do we leverage the resources and existing capabilities across the Department? How do we work most effectively with the private sector in this regard?

I mentioned earlier that doing something like the QHSR and the BUR takes nerves of steel. When we elevated cybersecurity to one of the five key missions of Homeland Security, there was quite a reaction—surprise.

Senator COLLINS. From whom?

Ms. LUTE. From a number of stakeholders across the country. Surprise—as if people had not really been thinking about it as an element of our homeland security. And so the simple articulation of the mission alone achieved a kind of effect we were hoping to achieve, which is to create a culture of awareness, a culture of responsiveness and engagement on this important and critical mission. So as we build out the Department's capabilities in this regard, again, understanding that we are largely an operational Department, we will prioritize what our requirements are in the 2012 budget.

Senator COLLINS. And, finally, I know that the Chairman brought up concerns about the Intelligence and Analysis Office's reliance on contractors. I want to talk about another issue with that office. A very important function of that office is to share information with State and local officials and first responders.

As you may be aware, the Appropriations Committee put a rider on the office that fences in some of the spending and, more troubling to me, attempts to limit what the office can do by saying that it should only produce reports that are unique—I am overstating it slightly, but it constrains the ability of the office to serve its customers because it says if there is any duplication, someone else should do it.

Have you looked at that language?

Ms. LUTE. I have, Senator.

Senator COLLINS. And do you have concerns about it?

Ms. LUTE. I do have concerns, Senator. The value proposition of our I&A office is to equip the homeland security enterprise with the information and intelligence it needs throughout the whole enterprise, including State and local officials, and that important, as the Chairman mentioned earlier, two-way sharing of information is so essential to the discharge of our missions.

Senator COLLINS. I would strongly encourage you and the Secretary to put your concerns in writing to Senators Dianne Feinstein and Christopher Bond, who initiated the proposal. Unfortunately, it was not cleared with our Committee, but we are going to work with the sponsors and with other members of the Appropriations Committee to try to clarify it. It would be helpful for us to have a letter from you expressing the concerns and for the appropriators to have it as well. And as someone who sits on both committees, as does Senator Voinovich, I think you can be assured that we would attempt to try to resolve these issues.

Ms. LUTE. Thank you.

Senator COLLINS. I will speak for myself actually on that, but I know the Chairman and I have discussed it.

Ms. LUTE. Thank you.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.



Chairman LIEBERMAN. Well, as usual, you can speak for me, too. I agree. It was actually a misunderstanding between me and one of the members of the Appropriations Committee, and I believe it was reflected at the Appropriations Committee markup that I supported this amendment, which I did not. And I am worried that it actually conflicts with existing law in terms of the authorities of the intelligence section of the Department of Homeland Security and will inhibit the capacity of the Office of Intelligence and Analysis at DHS to be of help to the Secretary, you, the other components of the Department, and most critically, as we have talked about, State and local law enforcement officials around the country.

So I think I am going to work with Senator Collins and our colleagues on the Committee on this, but I want to second her request that the Secretary and you send a letter to the appropriators to let them know that this is not a good move on their part.

Ms. LUTE. Thank you.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins.

I think we have cross-examined you enough generally within the Geneva Convention. I think we have not gone beyond those rules. Thanks for your effort on this. I think you have done a lot of constructive work, but on the BUR, the take-away is we really need more details. I think you are heading in a good direction, but it is hard for us to really judge until we see those implementing plans.

I gather that the third part of this three-part approach to the look forward is the details that will come with the fiscal year 2012 budget, right?

Ms. LUTE. Yes.

Chairman LIEBERMAN. And that is where you hope to show us how you are going to implement it.

Ms. LUTE. Exactly, Mr. Chairman. As I mentioned earlier, one of the lessons learned is that the timing of a QHSR exercise, like such as was envisaged, is important. And we are conforming to the budget submission process, and then that is, as we have spoken about over 18 months, the third part of the exercise.

Chairman LIEBERMAN. I really want to ask that as you make more specific the implementation plans for these 44 initiatives and enhancements, you send copies to Senator Collins and me, and we will circulate them to the Committee, so that we will not have to wait until the budget is submitted next year to understand how you are going forward with some of these.

Ms. LUTE. We look forward to working very closely with both of you and with the Committee.

Chairman LIEBERMAN. Thank you.

The record of the hearing will stay open for 15 days for additional statements and questions. With that, I thank you, Ms. Lute, and adjourn the hearing.

Ms. LUTE. Thank you.

[Whereupon, at 11:35 a.m., the Committee was adjourned.]



# APPENDIX

---

## Opening Statement of Chairman Joseph I. Lieberman

### *“Charting a Path Forward: The Homeland Security Department’s Quadrennial Homeland Security Review and Bottom Up Review”* July 21, 2010

The hearing will come to order. Good morning and welcome to the Deputy Secretary of the Department of Homeland Security, Jane Holl Lute. In the 9/11 Recommendations Act of 2007, Congress mandated that the Department of Homeland Security carry out a Quadrennial Homeland Security Review, a QHSR, as a way to develop and update strategies for homeland security within the federal government and ensure that the Department’s programs and activities were aligned with that homeland security strategy.

The Act required that the annual QHSR be provided to Congress by the end of 2009.

The QHSR was modeled on the Quadrennial Defense Review (QDR) that was put in place in the 1990s to ensure that the leaders of the United States military would focus on emerging national security threats, that to some extent the requirement to do the QDR would force them to look above the pressing events of the day, over the horizon to the challenges that were ahead and then to present to Congress and the public the strategies and resources to counter them.

The QHSR, which was completed in early February, and the follow-on Bottom Up Review – or BUR – which was completed and issued just a few weeks ago are meant to serve the same purpose for homeland security. They have the potential to be the catalyst for ongoing transformation and improvement of the Department, as well as across our entire homeland security community outside of the Department. In that sense we’re very fortunate to have Secretary Lute with us because I know that you oversaw these two reports.

This morning we want to hear about the results of this process, including the impact that it is having on strategic planning more broadly within the Department and at other homeland security agencies.

I’d like to hear about the steps that will be taken to implement the initiatives described in the report – including how it will impact the Department’s budget priorities in future years and how the Department intends to work with Congress on initiatives that may require statutory changes.

Forty-four initiatives are described in the BUR report, the Bottom Up Review, in areas such as information-sharing, management integration, DHS regional alignment, and the organizational framework for cybersecurity. In fact, cybersecurity—in a noteworthy change—has now made its way into the top five mission areas of the Department of Homeland Security and I applaud that placement because that’s exactly where I think it belongs.

The BUR is also a broad narrative of the Department's key missions, too broad at least in its first iteration and various of its parts, and its goals for improving those missions, which sometime in the reports were too vague to me as I read them. I hope, Madam Secretary, that you'll be able to develop those in some more detail today.

When Congress created the Department of Homeland Security out of 22 different federal agencies in 2002, we knew it would take time for it to mature into a cohesive agency that could focus its many parts on its two main missions – take the lead in our nation's fight against the Islamist terrorists who attacked us on 9/11 and then be able to respond better to natural disasters. And overall as I've said here many times, the Department has done very well at achieving those missions, but it still has a way to go as we all acknowledge.

The QHSR and the BUR are important steps on the path to achieving that goal and I have questions that I'm going to ask about that.

I do want to say that we hold this hearing against the backdrop of a series of articles that's been in "The Washington Post" called "Top Secret America" that examines the new institutions and programs created after 9-11, particularly focused on intelligence, but also including the Department of Homeland Security. So it makes this oversight of the QHSR and the BUR particularly timely.

The Post series has raised important questions about the big changes in our government since 9/11.

For instance: Is too much of our war against the terrorists who attacked us on 9/11 being out-sourced to private contractors? That's a big question raised by the Post series and one that has been a concern of this Committee for some significant period of time.

Going back to October of 2007, we held a hearing on the Department's reliance on contractors. At that hearing, the GAO presented the results of a review that they conducted at the request of Senator Collins and myself. We've consistently pressed the Department on this issue in the context of oversight of specific programs, such as SBInet and cybersecurity for example, where there continue to be a number of private contractors involved. The former Under Secretary for Management Elaine Duke I think tried to dig into this issue towards the end of the last administration, but didn't get very far and I'm not sure there was support from people above her.

I am pleased to say that it does seem to me that a review of the contractor workforce is underway now under Secretary Napolitano and Deputy Secretary Lute. At a briefing in December, we heard for the first time that DHS is trying to quantify the number of contract employees. The numbers that we've received are really quite remarkable. At an oversight hearing on this question a while ago, I was shocked to hear the number 200,000 contract employees working for the Department of Homeland Security, as compared to 188,000 full-time civilian employees.

After the hearing, Senator Collins and I wrote to Secretary Napolitano to ask for a more detailed breakdown on the contractor work force so we could determine whether those contract

employees were doing inherently governmental work, in violation of the law. It's hard to imagine with so many of them that some of them were not and I think we've got to face that and deal with it so that the reality comes into performance with the law.

While we have been assured repeatedly by the department that a review is underway, we still as of this morning don't have a timetable for when that review will be complete or a specific breakdown at the program level of the current full-time employee to private contractor ratios.

I hope, Secretary Lute, that you'll be able to help us answer some of these questions today, and if not today then as soon as possible. While, in my opinion, a lot of the growth of the homeland security and intelligence community of the U.S. government after 9/11 was necessary and I don't know if the series in the Post intends to say that the system is out of control, I don't find from my inquiry that it's out of control, both because of the mission of the Department and also because of the creation of the Director of National Intelligence doing the same.

But there's been a lot of growth, it happened quickly and it's part of why we've been relatively fortunate since 9/11, thank god, and thanks to all the people who have helped us do that, that we have not been hit again with anything like 9/11. But the facts in the Post series, and all that we've been working on over the past three years here in the Committee, say that we can't just let the machine operate without control from the executive branch and oversight from the legislative branch so that we make sure that we're spending taxpayer dollars in a cost-effective way.

I look forward to discussing this and all the other topics that the QHSR and BUR raise with you this morning. I appreciate you being here.

**Opening Statement of  
Senator Susan M. Collins**

**“Charting a Path Forward: The Homeland Security Department's  
Quadrennial Homeland Security Review and Bottom-Up Review”  
July 21, 2010**

Thank you, Mr. Chairman, for holding this hearing on the need to establish clear priorities for the Department of Homeland Security, the federal entity created to help protect our country from terrorism and other threats. As has been stated many times, if you try to protect everything, you end up protecting nothing. So, it is incumbent upon the Department – particularly when budgets are tight – to set detailed priorities to improve the preparedness and security of our nation.

The Department's Quadrennial Homeland Security Review (QHSR) was a good first attempt to outline strategic homeland security missions and goals.

Yet, the Department acknowledged that the QHSR was incomplete, so it conducted a follow-on review. This assessment, known as the “Bottom-Up Review” (BUR) was intended to set priorities for security initiatives and reorganization at the Department.

While I appreciate the Department's effort to undertake such a comprehensive analysis, the results are disappointing. Indeed, the two reviews simply don't compare to the level of planning and analysis that goes into the Quadrennial Defense Review and supporting documents.

For example, in the QDR and the Navy's shipbuilding plan, the Department of Defense outlines specific measurable goals – such as a 313-ship Navy. The 30-year shipbuilding plan includes a force structure, construction plan, funding assumptions, and specific articulation of risk inherent in the force projections.

By comparison, the QHSR and BUR amount essentially to high-level strategy documents that provide little in the way of concrete goals or the actions needed to achieve them.

For example, the reviews set some DHS goals to eliminate unnecessary duplication, to decrease operational inefficiencies, and to promote cyber security. But, without specific, measurable plans, how does Congress hold the Department accountable for meeting these goals?

In these documents, the Department highlights the critical need to address the threat of a cyber attack and indeed lists cyber security as one of its five strategic "pillars." Nevertheless, the President's budget request for fiscal year 2011 cut the Department's cybersecurity budget by \$19 million. How can the Department shoulder even the general responsibilities of an entire "pillar" while cutting the associated budget? The documents do not explain this contradiction, nor outline how the Department plans to do more with less.

As co-author with the Chairman and Senator Carper of comprehensive and bipartisan cyber security legislation, I am disappointed that these reviews do not identify the authorities and resources that DHS will need to enhance its cyber security capabilities. The legislation this Committee approved last month would fill that gap.

The BUR also fails to provide any specificity on how the Department will reduce its overreliance on contractors. I have raised this concern with the Secretary repeatedly. A recent Washington Post investigation revealed that "six out of 10 employees" at the DHS Office of Intelligence and Analysis are from private industry. This is on top of the revelation that an astonishing 50 percent of the DHS workforce are contractors. This is unacceptable.

While contractors play an important role in augmenting the federal workforce, they cannot displace it. But what does the DHS report say? Simply that "DHS will continue to build on [contractor conversion] efforts at an even more aggressive pace . . . ." That is not a plan; it's a platitude.

Like a compass, the QHSR should aid the Department in aligning its budget requests with homeland security priorities. And, in turn, these priorities would help Congress evaluate the President's budget requests against measurable goals.

The reviews that the Department has presented to Congress accomplish none of these tasks - they do not include a budget plan for the Department nor assess how the organizational structure can better meet the national homeland security strategy.

The QHSR also slights the strategic threat posed by violent Islamist extremists by refusing to call that real and present danger what it is. This is ironic considering that the introduction to the QHSR discusses the Christmas Day attack - an attack conducted by a violent Islamist extremist.

The Review does not reference "violent Islamist extremism" or any variation of that phrase in the entirety of its 108 pages. And it refers to

"homegrown extremists" only once. That is astonishing given the alarming increase in the number of homegrown terrorist plots last year. In sharp contrast, the October 2007 *National Strategy for Homeland Security* uses the word "Islamic" 15 times and the word "homegrown" eight times.

The BUR fails to describe how the Department will confront the threat of home-based terrorism. If DHS does not acknowledge the nature of the threat or explain how the Department intends to counter it, Congress and the American people cannot judge how the Department's counterterrorism efforts are reflected in its budget and priorities.

I look forward to hearing from the Department's Deputy Secretary about how more concrete and actionable plans will be developed. Such planning is necessary to improve the efficiency of Department operations and to build sensible budget plans. Only then will the time and effort spent on these reviews pay dividends in the form of a usable roadmap to better protect the American people.





**Testimony of  
The Honorable Jane Holl Lute  
Deputy Secretary  
U.S. Department of Homeland Security**

**Before the  
Senate Committee on Homeland Security and Governmental  
Affairs  
July 21, 2010**

Good morning Chairman Lieberman, Ranking Member Collins, and members of the committee. It is my distinct honor to appear before you today to discuss the Quadrennial Homeland Security Review (QHSR) and Bottom-Up Review (BUR), and in particular how the Department of Homeland Security (DHS) plans to implement the initiatives set forth in these two efforts; how they will improve the performance of DHS and enhance the nation's homeland security; and lessons learned that can inform the next QHSR.

As you know, the submission of the QHSR Report to Congress on February 1, 2010 marked an important first step in a multi-step process to examine and address fundamental issues that concern homeland security. The QHSR Report described the Nation's homeland security interests, identified the critical homeland security missions, and defined a strategic approach to those missions by laying out the principal goals, essential objectives, and key strategic outcomes necessary for that approach to succeed.

The bottom-up review (BUR) was initiated in November 2009 as an immediate follow-on and complement to the congressionally mandated QHSR with the aim to align the Department's programmatic activities and organizational structure with the broader mission sets and goal identified in the QHSR. The BUR Report reflects that endeavor and represents an intermediate step between the QHSR Report and the DHS FY 2012-2016 Future Years Homeland Security Program (FYHSP), which will propose specific programmatic adjustments based on the QHSR strategic framework. Together, these three elements—the QHSR, the BUR, and the DHS FY 2012-2016 FYHSP—will address the primary legislative requirements set forth in Section 707 of the Homeland Security Act.

#### The QHSR

The QHSR resulted in a new strategic framework and a positive, forward-looking vision for homeland security: *A homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.* The QHSR strategic framework grounds homeland security in five missions and their associated goals and objectives, informed by a new conception of homeland security that places emphasis on: (1) the homeland security enterprise; (2) a more comprehensive and complete understanding of homeland security threats; and (3) the need to achieve balance across efforts related to Security, Resilience, and Customs and Exchange.

<b>Mission 1: Preventing Terrorism and Enhancing Security</b> <ul style="list-style-type: none"> <li>• Goal 1.1: Prevent Terrorist Attacks</li> <li>• Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities</li> <li>• Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events</li> </ul>
<b>Mission 2: Securing and Managing Our Borders</b> <ul style="list-style-type: none"> <li>• Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders</li> <li>• Goal 2.2: Safeguard Lawful Trade and Travel</li> <li>• Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations</li> </ul>
<b>Mission 3: Enforcing and Administering Our Immigration Laws</b> <ul style="list-style-type: none"> <li>• Goal 3.1: Strengthen and Effectively Administer the Immigration System</li> <li>• Goal 3.2: Prevent Unlawful Immigration</li> </ul>
<b>Mission 4: Safeguarding and Securing Cyberspace</b> <ul style="list-style-type: none"> <li>• Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment</li> <li>• Goal 4.2: Promote Cybersecurity Knowledge and Innovation</li> </ul>
<b>Mission 5: Ensuring Resilience to Disasters</b> <ul style="list-style-type: none"> <li>• Goal 5.1: Mitigate Hazards</li> <li>• Goal 5.2: Enhance Preparedness</li> <li>• Goal 5.3: Ensure Effective Emergency Response</li> <li>• Goal 5.4: Rapidly Recover</li> </ul>

The QHSR outlined this strategic framework to guide the activities of the members of the homeland security enterprise toward a common end.

#### **The BUR**

The BUR is the second major step of a three-step process that began with the QHSR and will culminate in the President's Fiscal Year 2012 budget request and the accompanying Fiscal Year 2012-2016 FYHSP. The BUR provided a DHS-specific review of the Department's responsibilities and authorities within each homeland security mission set forth in the QHSR, and the programs and activities required to effectively execute the Department's responsibilities within those missions. As required by the QHSR statute, the BUR included an assessment of the organizational alignment of the Department with the homeland security missions—including the Department's organizational structure, management systems, procurement systems, and physical and technical infrastructure—and a review and assessment of the effectiveness of the mechanisms of the Department for turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan for the Department.

The BUR had four specific aims:

- (1) To gauge how well current activities and departmental organization align with mission priorities and goals as outlined in the QHSR;

- (2) To identify ways to achieve better programmatic and budgetary alignment across the entire department;
- (3) To identify areas for enhanced mission performance; and
- (4) To prioritize initiatives to strengthen existing programs and organization, address shortfalls, and establish a foundation for innovation and advancement.

While the robust portfolio of DHS's component agencies could not be completely represented in a 40-page report, the BUR Report discusses the Department's core role in each of the homeland security missions, considers the additional statutory responsibilities of DHS component agencies, and outlines enhancements and initiatives that address three principal areas of emphasis:

- **Strengthening and Maturing DHS**—There is a need to strengthen the Department's ability to execute its mission responsibilities, run itself, and account for the resources that have been entrusted to it.
- **Enhancing Partner Capability and Capacity**—Responsibilities for homeland security extend beyond DHS and indeed, beyond the Federal government. For that reason, there is a need to strengthen the ability of partners in the homeland security enterprise—in particular, State, local, tribal, and territorial governments, and the private sector—to execute important aspects of core homeland security mission activities.
- **Deepening International Engagement**—Security of our homeland begins far from our shores. We must work with key international partners to improve the critical partnerships and activities that affect the homeland security mission space, consistent with the broad range of U.S. Government international priorities and in consultation and coordination with the Department of State and the U.S. Chiefs of Mission stationed in foreign countries.

#### **The BUR Process**

Beginning in November 2009, each DHS directorate, component, and office subdivided its programs into activities, and categorized those activities as mission activities, mission support activities, or business support activities. Each mission activity was then given a primary mapping to one of the five homeland security missions articulated in the QHSR Report, as well as to one of the six functional capability portfolios set forth in the Homeland Security Enterprise Architecture.<sup>1</sup>

The activities inventory resulted in a comprehensive catalogue of DHS activities across the homeland security missions. The three basic aims of the activities inventory were to: (a) increase comparability within and across Components; (b) improve measurement of mission outcomes and the contribution of particular programs to those outcomes; and (c) attain better cost

<sup>1</sup> The six functional capability portfolios in the Homeland Security Enterprise Architecture are Screening, Securing, Law Enforcement, Domain Awareness, Benefits Administration, and Incident Management. These mappings were done to facilitate functional capability portfolio reviews that are being conducted separately from the BUR.

estimating of missions, programs, and activities. The activities alignment allowed DHS leadership to view the full panoply of DHS activities within each mission, in order to enhance the accomplishment of the mission priorities identified in the QHSR through alignment and prioritization of DHS programs and resources.

As the activities inventory progressed, Department leadership began identifying policy, legislative, and organizational implications arising out of the QHSR mission goals and objectives and the activities inventory. I personally held several meetings with the leadership of the Department's directorates and operating components, as well as key offices, to discuss priority initiatives and enhancements in each of the five homeland security missions, as well as in the categories of Improving Department Management and Increasing Accountability. Those meetings resulted in an initial list of over 300 potential initiatives and enhancements. Through further discussion and analysis, that list was reduced to the 44 initiatives and enhancements that are described in the BUR Report.

### **BUR Results**

The BUR resulted in priorities across three main categories: (1) Enhancing Mission Performance; (2) Improving Department Management; and (3) Increasing Accountability. It should be noted that these are *four-year priorities*; DHS will not accomplish all 44 of the initiatives and enhancements in Fiscal Year 2012. Instead, DHS will begin work on the highest-priority initiatives now, propose the initiation of others in the President's Fiscal Year 2012 budget proposal, and accomplish others through the Fiscal Year 2012-2016 time frame of the FYHSP.

### **Enhancing Mission Performance**

#### *Mission 1: Preventing Terrorism and Enhancing Security*

Protecting the United States and its people from terrorism is the cornerstone of homeland security. DHS shares leadership roles and responsibilities in the U.S. government's efforts to prevent terrorist attacks with several Federal departments and agencies. DHS's responsibilities focus on three goals: preventing terrorist attacks; preventing the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear (CBRN) materials and capabilities within the United States; and reducing the vulnerability of critical infrastructure, key leadership, and events to terrorist attacks and other hazards. To improve performance in this mission area, the Department will:

- Strengthen counterterrorism coordination across DHS;
- Strengthen aviation security by bolstering the international aviation security system, improving security processes and technologies, and encouraging partnerships with industry;
- Create an integrated Departmental information sharing architecture and link that architecture to interagency efforts to prevent terrorism while protecting privacy, civil rights and civil liberties;

- Deliver infrastructure protection and resilience capabilities to the field, in conjunction with efforts to “design in” greater resilience in critical infrastructure;
- Set national performance standards for identification verification;
- Increase efforts to detect and counter nuclear and biological weapons and dangerous materials;
- Standardize and institutionalize the National Fusion Center Network;
- Promote safeguards for access to secure areas in critical facilities, including through increased risk-informed screening and recurrent vetting;
- Establish DHS as a center for excellence for canine training and deployment; and
- Redesign the Federal Protective Service to better match mission requirements.

*Mission 2: Securing and Managing Our Borders*

DHS is responsible for secure, well-managed borders that not only protect the United States against threats from abroad, but also expedite the safe flow of lawful travel and commerce. Achieving this outcome rests on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations. To strengthen efforts to achieve these goals, the Department will:

- Expand joint operations and intelligence capabilities, including enhanced domain awareness;
- Enhance the security of the global trade and travel systems responsible for the secure movement of people and goods, including enhanced container and maritime security and prioritization of immigration and customs investigations relating to global trade and travel systems;
- Strengthen and expand DHS-related security assistance internationally (e.g. border integrity and customs enforcement security assistance) consistent with U.S. government security and foreign assistance objectives in consultation and coordination with the Departments of State and Defense; and
- Work closely with the governments of Canada and Mexico to enhance North American security.

*Mission 3: Enforcing and Administering Our Immigration Laws*

Smart and effective enforcement and administration of our immigration laws allows the government to facilitate lawful immigration while identifying and removing those who violate our laws. To support this mission area, DHS will:

- Pursue comprehensive immigration reform;
- Strengthen and improve the Department's immigration services process;
- Prioritize national security and fraud detection vetting in immigration services processes;
- Target egregious employers who knowingly exploit illegal workers;
- Dismantle human smuggling organizations through concerted law enforcement activity;
- Improve the detention and removal process by increasing non-investigatory law enforcement staffing and expanding Secure Communities and the Criminal Alien Program;
- Work with new Americans so that they fully transition to the rights and responsibilities of citizenship; and
- Build and maintain a model immigration detention system.

*Mission 4: Safeguarding and Securing Cyberspace*

Cyber infrastructure forms the backbone of the Nation's economy and connects every aspect of our way of life. While the cyber environment offers the potential for rapid technological advancement and economic growth, a range of malicious actors may seek to exploit cyberspace for dangerous or harmful purposes, disrupt communications or other services, and attack the Nation's infrastructure through cyber means. By statute and Presidential directive, DHS has the lead for the Federal government to secure civilian government computer systems, works with industry to defend privately-owned and operated critical infrastructure, and works with State, local, tribal and territorial governments to secure their information systems. In pursuing these initiatives and enhancements to strengthen the Department's capabilities in cybersecurity, DHS will:

- Better integrate and focus DHS cybersecurity and infrastructure resilience operations;
- Strengthen DHS's ability to protect cyber networks;
- Increase predictive, investigative, and forensic capabilities for cyber intrusions and attacks; and
- Promote cybersecurity public awareness through the cyber awareness program and the planned implementation of a national public awareness and education campaign.

*Mission 5: Ensuring Resilience to Disasters*

Ensuring domestic resilience to disasters is grounded in the four fundamental elements of emergency management: mitigating hazards, increasing our Nation's preparedness, effectively responding to emergencies, and supporting community recovery. During domestic disasters, the Department's role, largely executed through the Federal Emergency Management Agency

(FEMA), is principally one of coordinator, working closely with our State, local, regional, tribal, and territorial partners, as well as nongovernmental organizations and the private sector, to enhance preparedness, build and sustain capabilities, and act as an aggregator of resources from across the Federal government. DHS, through FEMA, also has specific direct responsibilities, including disaster preparedness, response, recovery, and mitigation, including field coordination, disaster logistics, individual and public assistance programs, as well as national continuity programs. DHS maintains a significant first responder capability for disasters in the maritime domain through the U.S. Coast Guard (USCG), and also ensures the resilience of critical infrastructure to disasters through the National Protection and Programs Directorate. In order to strengthen mission performance, DHS will:

- Enhance catastrophic disaster preparedness through shared objectives and capability standards at the Federal, State, local, regional, tribal, territorial, nongovernmental, and private sector level, developed in close collaboration with all partners and based on planning assumptions that address risk-based worst case scenarios (maximums of maximums);
- Improve the capabilities of DHS to lead in emergency management through a new strategic approach to developing FEMA's workforce, creating an emergency management career path, and harmonizing emergency responder training across DHS;
- Explore opportunities with the private sector to "design-in" greater resilience for critical infrastructure; and
- Make individual and family preparedness and critical facility resilience inherent in community preparedness.

#### **Complementary Department Responsibilities and Hybrid Capabilities**

DHS also performs a number of services and functions that are complementary to its homeland security mission responsibilities, including marine safety, stewardship, and environmental protection, and certain categories of law enforcement activities. These services and functions are typically performed with hybrid capabilities—assets and resources capable of performing multiple missions—which are a hallmark of homeland security. For example, the same assets and personnel that patrol our borders, enforce our immigration laws, and respond to major oil spills also enforce safety regulations, assist travelers, and safeguard natural resources. These complementary activities are critical to fulfilling other national interests and are often intertwined with and mutually supporting of homeland security activities.

#### **Improving Department Management**

The integration of 22 different Federal departments and agencies into a unified, integrated Department of Homeland Security continues to represent a significant public policy and management challenge. Over the course of its brief history, DHS has evolved to its current structure, which includes seven operating components, four headquarters directorates, and over 15 additional supporting offices, many of which combine responsibilities for policy,



management, operations, acquisition, external affairs, and research and development. In order to improve department management, DHS proposes to:

- Seek restoration of the Secretary's reorganizational authority for DHS headquarters to address new threats and realize greater efficiencies;
- Realign component regional configurations into a single DHS regional structure;
- Improve cross-Departmental management, policy, and functional integration;
- Strengthen DHS internal counterintelligence capabilities and internal intelligence sharing and distribution;
- Enhance the Department's risk management capability;
- Invest in the DHS workforce and improve retention and morale by strengthening employee health and wellness and other human resources programs;
- Strengthen coordination within DHS through cross-Departmental training and career paths;
- Increase diversity in the DHS workforce, especially at senior levels; and
- Balance the DHS workforce by ensuring strong federal control of all DHS work and reducing reliance on contractors as needed to enhance competency and meet long-term mission requirements.

#### **Increasing Accountability**

To enhance mission performance and improve Departmental management, DHS must increase accountability across the organization. While accountability cuts across all aspects of the organization's operations, our initial focus will be to maximize the performance and resource data we collect to support strategic and risk-informed decision-making. The initiatives described below are intended to improve the effectiveness of the Department in turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan. DHS proposes to:

- Increase its analytic capability and capacity by enhancing strategic planning, resource allocation, risk analysis, net assessment, modeling capabilities, statistical analysis, and data collection;
- Improve performance measurement and accountability by increasing the quality of the Department's performance measures and linking those measures to the mission outcomes articulated in the QHSR Report; and
- Strengthen acquisition oversight by strengthening the Department's independent cost estimation capability.

### **Implementing the BUR and the Path Forward**

BUR implementation began on April 19 with the submission of resource allocation plans by DHS directorates, components, and offices. The resource allocation plan submission process was restructured to show resources in a common set of expenditure categories according to the activities identified in the BUR. By collecting the data in this way, DHS has been able to systematically look at costs associated with salaries (people), expenses, investments (planning, acquisition, and maintenance), research and development, and assistance payments (grants) across components, which DHS has never been able to do before. From this, DHS directorates, components, and offices were able to construct a more unified FYHSP program structure based on the activities. That programmatic structure facilitates much easier evaluation of resource prioritization and a clearer understanding of the alignment of program outcomes with the overall mission goals and objectives set forth in the QHSR Report. DHS is currently evaluating the resource allocation plans through its Program Review Board, and the final decisions on the resource allocation plans will ultimately be set forth in the President's Fiscal Year 2012 budget proposal and the accompanying Fiscal Year 2012-2016 FYHSP.

In addition, each of the 44 initiatives and enhancements set forth in the BUR Report have been assigned to a DHS directorate, component, or office, to lead Department-wide efforts to implement the initiative. Some of the initiatives will require programmatic or budgetary activity, and the Administration's proposals for those initiatives will be included in the President's Fiscal Year 2012 budget proposal and the accompanying Fiscal Year 2012-2016 FYHSP. Other initiatives involve policy, legislative, and organizational activities. DHS will evaluate policy alternatives and change policy as appropriate, and those legislative and organizational proposals for Fiscal Year 2012 will be proposed either within the President's Fiscal Year 2012 budget proposal and the accompanying Fiscal Year 2012-2016 FYHSP or another venue as appropriate.

DHS will also undertake, in coordination with appropriate interagency partners, additional efforts in support of the QHSR, including the development of requirements for intelligence, science and technology, support to civil authorities, and other elements described in the QHSR and BUR reports.

### **Lessons Learned**

As we look toward the next QHSR, I would like to share with you a few lessons learned. First, future QHSRs should not be conducted in transition years. Senior leadership engagement and support is critical to any planning process of this scale, and the timeline of the transition process creates significant challenges in the critically important conceptualization and launch phases of a review. Based on the foundation set by the 2009 QHSR, the next QHSR will involve significant analytics during both the preparatory and early phases of the review, which must be conducted with full buy-in and awareness of senior leadership.

In addition, the other major quadrennial reviews, including the Quadrennial Defense Review and Quadrennial Diplomacy and Development Review, among others, must be synchronized. Today's security environment demands whole of government solutions and flexible and adaptable policy responses to difficult challenges. Quadrennial reviews offer an important opportunity to pause and ensure the strategy is right and the organization is aligned. We must

find ways to do this in a way that meaningfully leverages the knowledge of each relevant department and agency, as well as stakeholders beyond the federal government.

Lastly, though the QHSR succeeded in breaking down bureaucratic and other barriers to large-scale engagement with the public, there is still more we can do. The technology and the tools are there for government to significantly enhance representative policymaking and we must facilitate the use of such tools across the government.

### **Conclusion**

Thank you again for the opportunity to speak with you today about implementation of the QHSR and DHS Bottom-Up Review, and lessons learned for the future. I look forward to your questions.

**Post-Hearing Questions for the Record  
Submitted to the Honorable Jane Holl Lute  
From Senator Joseph I. Lieberman**

***“Charting a Path Forward: The Homeland Security Department’s Quadrennial  
Homeland Security Review and Bottom-Up Review”  
July 21, 2010***

<b>Question#:</b>	1
<b>Topic:</b>	NHSS
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The provision of law mandating the QHSR required that the review should “delineate and update, as appropriate, the national homeland security strategy...” Does the QHSR report replace the National Strategy for Homeland Security issued by President Bush in October 2007, or is the QHSR a complementary document to it?

**Response:** The QHSR Report is currently the prevailing source of strategic guidance for homeland security. It establishes a mission-based strategic framework for homeland security based on five missions: Preventing Terrorism and Enhancing Security; Securing and Managing our Borders; Enforcing and Administering our Immigration Laws; Safeguarding and Securing Cyberspace; and Ensuring Resilience to Disasters. These five missions are the priority, critical homeland security missions of the Nation.

QHSR differs from previous strategy in four primary ways:

1. Outlines a comprehensive mission framework that captures the universe of homeland security activities in a rational and clearly understandable construct.
2. Incorporates critical homeland security mission activities that were not explicitly identified as part of homeland security in previous strategies—namely, immigration enforcement and administration; cybersecurity; and emergency management.
3. Broadens the understanding of homeland security threats and hazards to specifically include high-consequence weapons of mass destruction, Al-Qaeda and global violent extremism, mass cyber attacks, intrusions, and disruptions, pandemics and natural disasters, and illegal trafficking and related transnational crime; and
4. Shifts emphasis away from “Prevent, Protect, Respond, and Recover” as the primary strategic architecture towards the concepts of “Security, Resilience, and Customs and Exchange” upon which the foundations of homeland security rest.

<b>Question#:</b>	2
<b>Topic:</b>	recommendations
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Quadrennial Homeland Security Review was mandated by Section 2401 of the Implementing the Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53). Please provide your assessment of the feasibility of the following requirements of Section 2401, in light of the experience of carrying out the QHSR and BUR in 2009-2010, as well as any other recommendations for clarifications or improvements to the statute:

The timing of the review, due currently at the end of the first year of each Presidential term;

**Response:** Future QHSRs should not be conducted in transition years. Senior leadership engagement and support is critical to any planning process of this scale, and the timeline of the transition process creates significant challenges in the critically important conceptualization and launch phases of a review. Based on the foundation set by the 2009 QHSR, the next QHSR will involve significant analytics during both the preparatory and early phases of the review, which must be conducted with full buy-in and awareness of senior leadership.

**Question:** The requirement that the review be led by DHS but looking at homeland security broadly, beyond the scope of the missions and activities carried out by the Department of Homeland Security;

**Response:** Homeland security is most appropriately viewed from an enterprise perspective, reflecting the shared responsibility of Federal, State, local, tribal, territorial, nongovernmental, and private sector partners—as well as individuals, families, and communities—for ensuring a safe, secure, and resilient homeland.

**Question:** The requirement for a budget plan that provides sufficient resources to successfully execute the missions called for in the national homeland security strategy;

**Response:** The requirement for a budget plan to provide sufficient resources to execute homeland security missions is feasible and desirable. For DHS, that budget plan exists in the form of the DHS Future Years Homeland Security Program (FYHSP), which is a five-year budget plan. The QHSR guides development of the FYHSP.

**Question:** The requirement for a discussion of the status of cooperation among Federal

<b>Question#:</b>	2
<b>Topic:</b>	recommendations
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

agencies;

**Response:** A specific review of the status of Federal cooperation is a critical element to ensuring the Nation's homeland security; however, such a roles and missions review is most appropriately conducted by the White House and is beyond the scope of what DHS can complete in a strategic review. The concept of the homeland security *enterprise* established in the QHSR explicitly acknowledges the fundamental role that other Federal partners play in homeland security. The QHSR makes specific recommendations on how to strengthen and mature the homeland security enterprise, including mechanisms to enhance unity of effort across multiple homeland security partners and stakeholders.

**Question:** The requirement for a discussion of the status of cooperation between the Federal government and State, local and tribal governments in preventing terrorist attacks and responding to threats to national homeland security.

**Response:** A specific review of the status of Federal, State, local, and tribal government cooperation is a critical element to ensuring the Nation's homeland security; however, such a roles and missions review is most appropriately conducted by the White House and is beyond the scope of what DHS can complete in a strategic review. The concept of the homeland security *enterprise* established in the QHSR reflects explicit acknowledgment of the fundamental role that Federal, State, local, tribal, territorial, nongovernmental, and private sector partners—as well as individuals, families, and communities—play in homeland security. The QHSR makes specific recommendations on how to strengthen and mature the homeland security enterprise, including mechanisms to enhance unity of effort across multiple homeland security partners and stakeholders.

<b>Question#:</b>	3
<b>Topic:</b>	costs
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** How much did the Department spend to develop the QHSR and BUR, including costs related to (a) full-time headquarters personnel, (b) detailees and/or participants (reimbursable or non-reimbursable) from DHS components or other Departments or agencies, (c) use of Department FFRDC's, (d) use of other contractors, and (e) other costs? Please provide a detailed breakout of costs by activity, office, fiscal year, and segment of the process (i.e. distinguish between QHSR costs and BUR costs).

Did the Department have sufficient resources to carry out the QHSR and BUR in a way that would satisfy the statutory requirements of the review? If not, what steps is DHS taking or planning to take to more accurately estimate costs and budgetary requirements for the next QHSR?

**Response:** Office of Strategic Plans had responsibility for the funding and conduct of the Quadrennial Homeland Security Review. The following is a breakdown of the requested QHSR costs:

FY	HQ Personnel Costs	Intra/Inter Agency Personnel Costs	FFRDC (HSSAI)	Contractor Support	Total (FY)
2008	915,276	Not Tracked	434,575	739,795	<b>\$2,089,646</b>
2009	1,315,771	3,913,351	7,149,000	1,219,895	<b>\$13,598,017</b>
Total	<b>2,231,047</b>	<b>3,913,351</b>	<b>7,583,575</b>	<b>1,959,690</b>	<b>\$15,687,663</b>

Program Analysis and Evaluation had responsibility for conduct of the Bottom Up Review. The following is a breakdown of the requested BUR costs:

FY	HQ Personnel Costs	Intra/Inter Agency Personnel Costs	FFRDC (HSSAI)	Contractor Support	Total (FY)
2010	1,253,900	0	0	314,800	<b>1,568,710</b>

DHS applied sufficient resources to conduct these reviews and satisfy statutory requirements. DHS will program additional resources internally as needed for future reviews.

<b>Question#:</b>	4
<b>Topic:</b>	studies
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Please provide a complete list of studies and reports undertaken since January 2008 by DHS, and by external entities for DHS, in support of the QHSR and BUR, including the full name of the study, date of study, and the entity that produced the study, as applicable.

**Response:** The QHSR was supported by seven study groups. Four of the groups addressed the purpose and objectives of the four homeland security mission areas, and three of the groups analyzed mission support tools—namely, homeland security national risk assessment, homeland security planning and capabilities, and DHS strategic management. The study groups convened from May 2009 through September 2009 and resulted in specific recommendations that were then considered by senior leadership. These study groups, consisting of over 200 participants from 42 DHS directorates, components and offices, represented the core of the QHSR effort. The study groups were convened by the Office of Strategic plans and supported by the Department's Federally Funded Research and Development Center, the Homeland Security Studies and Analysis Institute (HSSAI).



<b>Question#:</b>	5
<b>Topic:</b>	plans
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** At the Committee hearing I requested copies of the 44 Strategic Implementation Plans that have been developed to implement the Bottom Up Review (BUR) findings and recommendations.

Please provide the Committee with copies of all of the 44 Strategic Implementation Plans, as requested at the hearing, and any overarching documents that outline the Department's timetable for implementation of these plans.

**Response:** The strategic implementation plans are an evolving product internal to the Administration. Each BUR initiative was tasked to a lead organization within DHS that developed one-page strategic implementation plan executive summaries, completed on July 2, 2010. That material was reviewed by DHS leadership and programmatic initiatives became the subject of Program Review Board deliberations throughout July as part of the DHS resource allocation process. Policy, organizational, and legislative initiatives are the subject of additional review by the Assistant Secretary for Policy and Under Secretary for Management throughout August. The programmatic implications of these initiatives will be evident in the Fiscal Year (FY) 2012 President's Budget submission in February, 2011, and in the associated five-year FY 2012-2016 Future Years Homeland Security Program (FYHSP).

<b>Question#:</b>	6
<b>Topic:</b>	report
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** Section 874 of the Homeland Security Act requires that DHS submit to Congress a Future Years Homeland Security Program (FYHSP) at or about the same time as the annual budget request that provides a five-year budget outlook for key programs and activities of the Department. This report is intended to emulate the Future Years Defense Program (FYDP), which is a key source of information for the Armed Services Committee's efforts to pass a Defense Authorization bill each year. The FYHSP is similarly intended to give the Committee information that it needs in order to authorize funding for the Department.

This Committee did not receive an FYHSP report in 2009 to accompany the FY 2010 budget request. And this Committee has not yet received an FYHSP report this year to accompany the FY 2011 budget request. It is my understanding that these reports have been completed, but that decisions have been made to prevent their release to Congress, in contravention of Section 874 of the Homeland Security Act.

What is the current status of the FY 2010-2014 FYHSP report? What has prevented its release to date?

**Response:** The Administration released a FY 2010 Policy Budget to the Congress in February 2009 which was followed by a more complete congressional justification and President's Budget in May 2009. Typically, issuance of the FYHSP report would occur within 60-90 days following release of the President's budget. However, by the time the FY 2010-2014 FYHSP report was completed and reviewed with DHS leadership and OMB, a joint determination was made not to release the report. Given the timing, the report would have coincided with the Administration's review of FY 2011 budget justifications from Agencies, making the material in the report indicative of then ongoing pre-decisional budget deliberations for FY2011.

**Question:** What is preventing the release of the FY 2011-2015 FYHSP report? What has prevented its release to date?

**Response:** The FY 2011-2015 FYHSP report was completed and reviewed with DHS leadership and OMB in March, 2010. Unfortunately the timing of this report, shortly after the Quadrennial Homeland Security Review and in the midst of the Bottom-Up Review, did not allow incorporation of performance measures that adequately represent the

<b>Question#:</b>	6
<b>Topic:</b>	report
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Department's contribution to the new mission areas and program structure under development at that time.

**Question:** Please provide a copy of the current versions (as of the date of the submission of these questions) of the FY 2010-2014 and FY 2011-2015 FYHSP reports to the Committee. If you are unable or unwilling to provide these reports upon the receipt of this question, please explain the reasons why.

**Response:** The rationale for not releasing these reports is described above.

**Question:** How will activities undertaken as part of the QHSR and BUR process (including the BUR Activities Inventory) be used to improve or inform the FY 2012-2016 FYHSP and subsequent FYHSPs?

**Response:** The FY 2012-2016 FYHSP will include new performance measures developed over the course of the Bottom-Up Review which are reflective of the objectives of the Quadrennial Homeland Security Review. The Department-wide Activities Inventory will enable the Department to advance in three primary focus areas:

- o Comparability of our programs, activities, and resources within and across components;
- o Contribution of our programs, activities, and resources to mission outcomes; and
- o Alignment of activities to missions, identification of the cost elements/drivers of activities, aggregation of activity costs to programs and missions, and promotion of consistency between planned activities and execution.

The activities inventory provides visibility into the various activities that comprise the programs that contribute to the missions of the QHSR. It allows for new programs to be introduced in our Annual Performance Report and Fiscal Years (FY) 2012-2016 Future Years Homeland Security Program. The comparability and granularity provided will continue to be an important element required in the annual internal DHS resource allocation process and analysis provided by cross-Component issue teams in each year's Program Review.

<b>Question#:</b>	7
<b>Topic:</b>	approach
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** A recent report from the Homeland Security Institute (HSI), one of the Department's FFRDC's, indicates that "no method exists to determine what or how many strategic resources are needed to accomplish the goals and objectives" described in the QHSR, and adds that "no methodology has been designed to optimize these resources once they are defined." HSI is now developing a Capability and Capacity Model in response to this deficiency.

How great of a risk is it to the Department's effectiveness that it currently has no methodology for strategic resource allocation and optimization? What is the Department's approach to addressing this deficiency?

**Response:** While many DHS components have methodologies for determining needed capabilities and capacities in order to help guide strategic resource allocation, DHS has recognized that no standardized method exists across all missions. DHS is working to develop such a method, and the Homeland Security Institute (HSI) is playing a supporting role. This effort is intended to work in harmony with other analytic efforts across the Department, including the Risk Management and Analysis office's work on risk analysis and FEMA's work on national preparedness.

<b>Question#:</b>	8
<b>Topic:</b>	measurement
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The BUR lists as one of its priority initiatives as “Improve Performance Measurement and Accountability.” DHS has been working with OMB and GAO for years to develop better quality performance measures to assess how well the Department is fulfilling its mission, but so far its efforts have mostly fallen short.

What specifically does DHS plan to accomplish in this initiative and what is your timetable? What does DHS plan to have completed a year from now? In four years?

How are the efforts to improve performance measures as the result of the QHSR and BUR drawing on the Department’s ongoing dialogue and interaction with GAO on this issue?

**Response:** The Quadrennial Homeland Security Review (QHSR) strategic framework and the analytical work provided with the Bottom-Up Review (BUR) resulted in a large-scale effort to develop strategic-level performance measures that address contribution to the objectives of the QHSR. These outcomes delineated in the QHSR effort are the basis for driving towards a set of strategic performance measures. DHS leadership directed that the entire suite of measures be reexamined in light of this new strategy. Currently, 17 cross-Component teams are working to develop strategic-level measure across the 43 objectives of the QHSR, as well as evaluating and recommending changes to the existing measure suite. Teams are expected to report back to DHS leadership to provide new fully developed measures and measurement concepts in September 2010. Each of these measure proposals will have a timetable indicating how long it will take to begin official tracking on these measures. Some of these measures we will be able to implement immediately; others will take additional time to develop. Performance measure development is an ongoing and iterative process internally within DHS as we seek continuous improvement in how the Department assesses the effectiveness of programs. In addition to review by the department, OMB and GAO are both involved partners to review measures as they are developed.

<b>Question#:</b>	9
<b>Topic:</b>	program reviews
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In February 2010 the Committee requested copies of reports resulting from Program Reviews carried out by the DHS Office of Program Analysis and Evaluation. The After-Action Report for the Department of Homeland Security's FY 2010-2014 Program Review (available at <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA503010>) indicates that major reviews were carried out in areas such as People Screening, Cargo Screening, Interior Immigration Enforcement, Facilities Consolidation, Biowatch, IT, Intelligence, and Border Security.

Please provide the Committee with copies of reports resulting from these reviews, including on the topics mentioned above, and other similar program reviews conducted in the last three years.

**Response:** No formal reports were compiled. Program Reviews conducted as part of the internal DHS resource allocation process represent an internal pre-decisional deliberation among DHS leadership to help shape budget justifications for the Administration. These reviews resulted in a series of briefings covering each of the areas that set forth resource alternatives and tradeoffs. Executive Branch communications that led to the President's budgetary decisions are not disclosed by the agencies that prepared the budget.

**Question:** How are these reviews used by DHS to improve the effectiveness and efficiency of the Department's activities?

**Response:** The Program Review and analytical work of assigned cross-Component issue teams relate to major multi-year programmatic issues directed by leadership and are presented to the Program Review Board (PRB). The board is chaired by the Deputy Secretary and provides discussion/decision on alternative resource options and tradeoffs. These reviews increase cross-component coordination and communication which aid identification of gaps and overlaps in DHS activities across components as well as within components.

**Question:** How will the Activities Inventory developed as part of the Bottom-Up Review be used to support future Program Reviews within the Department?

<b>Question#:</b>	9
<b>Topic:</b>	program reviews
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Response:** The development of the Department wide Activities Inventory was one of the several tasks comprising the Bottom-Up Review to enable the Department to advance in three primary focus areas:

- o Comparability of our programs, activities, and resources within and across components;
- o Contribution of our programs, activities, and resources to mission outcomes; and
- o Alignment of activities to missions, identification of the cost elements/drivers of activities, aggregating activity costs to programs and missions, and promoting consistency between planned activities and execution.

The activities inventory provided a fresh look at the underpinning elements of the programs DHS uses to describe the outcomes it provides the public in the context of the missions detailed in the Quadrennial Homeland Security Review (QHSR) without presupposing whether the current structure is optimal. As a result you will see new programs introduced in our Annual Performance Report and Fiscal Years (FY) 2012-2016 Future Years Homeland Security Program. The comparability and granularity provided will continue to be important elements in the annual internal DHS resource allocation process and in the analysis provided by cross-Component issue teams in each year's Program Review.

<b>Question#:</b>	10
<b>Topic:</b>	timeliness
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In order for the Committee to conduct fair and constructive oversight over DHS, it is imperative that DHS provide timely responses to legitimate Committee inquiries. In particular, our oversight of DHS acquisitions requires the Department to provide us timely and detailed reports on the status of projects, as well as a clear understanding of DHS goals and its acquisition strategies. On March 23, Senator Collins and I wrote to the Secretary to ask a series of questions about CBP's plans for modernization of the Traveler Enforcement Compliance System, or TECS, a multi-year initiative, projected to exceed \$360 million, to modernize the database system used by CBP and ICE to manage law enforcement actions, including efforts to stop terrorists from traveling. In addition to mailing the letter, our staff circulated an electronic copy of the letter to DHS and CBP legislative affairs offices on March 23. Since March 23, our staff has repeatedly inquired about the status of a response, each time attaching another copy of the letter to the inquiry. We were dumbfounded to receive a response from the Executive Secretary dated July 22, stating that the letter was received on July 14, and indicating that the Department needed additional time to provide a detailed response.

Do you think it is acceptable for the Department to take nearly four months to respond to a letter from the Committee, and then to inform the Committee that the Department requires additional time to formulate a response?

When can the Committee expect to receive a response to our March 23 questions about the TECS modernization initiative?

How can the Committee have confidence that the Department is addressing weaknesses in its acquisition system when it takes longer than four months to provide fundamental information on its major acquisitions?

**Response:** DHS agrees that TECS modernization is a critical project and assures you that the DHS is closely monitoring it to ensure that the critical functions provided by TECS are successfully improved and extended into the future. Attached is a white paper with specific answers regarding the TECS modernization.



**U.S. Department of Homeland Security  
U.S. Customs and Border Protection  
Answers regarding the TECS modernization**

**Program Management Office Staffing**

Both the DHS Chief Information Officer (CIO) and Acquisition Program Management Division (APMD) provide oversight to the performance of the TECS modernization program and its program management office (PMO). The DHS CIO and APMD staffs interact with the PMO on an ongoing basis in addition to the formal reviews conducted by each office. Based on the concern expressed by the DHS CIO, U.S. Customs and Border Protection (CBP) developed a staffing plan that included adding more government staff and reducing the number of contractor staff. CBP has implemented a staff increase according to the plan with periodic updates to the DHS CIO. The TECS modernization PMO currently consists of 43 staff members, of which 10 are government employees.

**Contracting Strategy**

CBP revised the contracting strategy and is focusing on obtaining two long-term contracts. Over the last eight years, the application work within CBP's Passenger System Program Office (PSPO) has expanded beyond TECS, while the TECS system has also expanded through programs such as US-VISIT and the Western Hemisphere Travel Initiative. Based on the tremendous growth of the PSPO systems, a strategy was developed to divide the PSPO work among four application services contracts and an overarching project support contract. The four application services contracts would have divided the work into logical divisions, while the overarching contract would provide the project support for all PSPO work, including requirements management, processes, configuration management, and security for all the PSPO application work.

CBP also recognized that having four application services contracts would require a great deal of coordination and increased the risk for key interfaces and interdependencies between projects. For these reasons, CBP decided to change this strategy and pursue one large application services contract to handle all PSPO application work including TECS modernization. This will provide CBP with one contract for closely-related application efforts. However, CBP will award a separate contract for project support, as originally planned, which will include requirements management, processes, configuration management, and security for the PSPO application work. A separate contract for project support activities is critical to maintaining quality control, as it provides a separation of duties between the application development contractor and the project support contractor.

**Governance and Oversight**

TECS modernization oversight is provided both by DHS and CBP:

- The DHS CIO provides technical architecture oversight to the program through reviews at each stage of the lifecycle. TECS modernization has been through these reviews and

August 2010

received approval. Additionally, the DHS CIO conducted a special review of the technical approach of TECS modernization before the DHS Acquisition Review Board in September 2009. The DHS CIO concurred with the technical approach and CBP is currently addressing recommendations made by the DHS CIO.

- The DHS Chief Procurement Office (CPO) provides support and oversight for the procurement activities. The DHS CPO provides guidance and review, and will have final approval of the request for proposal for the TECS modernization contract before it is released to vendors to bid on.
- The DHS Acquisition Review Board reviewed the CBP TECS modernization in September 2009. The overall program received approval for Acquisition Decision Event (ADE) 1, which provides the overall authority to proceed with the program. Based on completing the action items outlined in the Acquisition Decision Memorandum (ADM), the Secondary Inspection was approved for ADE 2A/2B, which allows them to complete development and deploy to five sites for conducting operational testing and evaluation. High Performance Query received an ADE 2A approval which allowed for development activities to begin. The ADM from the Acquisition Review Board is enclosed. The CBP TECS modernization is scheduled for another Acquisition Review Board in September 2010.

As part of the acquisition review process within DHS Headquarters, the CBP has prepared all the documents required for acquisition approval. DHS Headquarters has approved the Test Evaluation Master Plan. Additionally, CBP has approved the Mission Needs Statement and it is being reviewed for final approval. The other required documents are currently in CBP's signature process and should be submitted to DHS Headquarters in late August. The acquisition documents provide the overarching requirements and plans for TECS modernization.

- The TECS Modernization Executive Steering Committee (ESC) is co-chaired by the CBP Deputy Commissioner, the Deputy Assistant Secretary of U.S. Immigration and Customs Enforcement (ICE), and the Deputy Director of U.S. Citizenship and Immigration Services (USCIS). ESC ensures the appropriate strategic business needs are addressed and the program is on course to deliver essential functionality in a timely and cost effective manner. ESC also sponsors the Integrated Governance Committee (IGC), which has members from all the major TECS modernization stakeholders, including CBP, ICE, USCIS, other DHS Components, the Department of State, and the Federal Bureau of Investigation. The IGC's purpose is to ensure no degradation of TECS functionality during the modernization effort by facilitating cross organization dependencies and change management along with high level program risk mitigation and communications.

### **Conclusion**

The TECS modernization effort is following all of the established review and decision protocols within both CBP and DHS Headquarters. These reviews ensure the program is being correctly monitored and administered. TECS modernization is proceeding on a sound, realistic plan to bring critical TECS functionality into a sustainable technology for the future. DHS will continue to closely monitor TECS modernization.

<b>Question#:</b>	11
<b>Topic:</b>	HQ services
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The BUR report indicates that “DHS will examine the creation of a Headquarters Services Division within the Management Directorate from the existing service functions of the business chief that will provide day-to-day business support functions to DHS headquarters elements.”

What are the key criteria that will be evaluated in the process of deciding on whether to create a Headquarters Services Division? What is the timeline for this evaluation?

If the Department decides to create a Headquarters Services Division, what statutory changes (if any) would be needed to facilitate its development?

**Response:** Subsequent to the BUR report identifying the need for an increased focus on service functions of the Management business chiefs, the Under Secretary for Management has created the Management Service Council (the Council) to foster integration and communication between management service providers for the purpose of improving service to Headquarters customers. Service areas include acquisition and procurement; human capital and human resources management; accounting and financial management; information technology; employee and physical security; and facilities, property, equipment, and other administrative services. The Council is chaired by the Deputy Under Secretary for Management and includes Executive Directors responsible for providing the day-to-day business support functions. Specifically, the Council will do the following:

- Assist management in implementing a service-oriented framework and fostering an organizational environment that supports the provision of efficient, effective management services;
- Serve as a forum to convey information and to discuss issues of mutual concern; and
- Work together and coordinate efforts to resolve common challenges and address issues.

The coordinated council approach will provide senior management level oversight and accountability regarding the provision of operational services to Headquarters offices. No additional statutory changes are needed to institute this approach to managing service delivery business functions.

<b>Question#:</b>	12
<b>Topic:</b>	career paths
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The BUR report states that “DHS will strengthen Department unity by developing DHS career paths that provide mobility within the Department and span headquarters and operational components.”

What are the most significant impediments to career mobility within the Department today?

**Response:** The most significant impediments to career mobility within the Department today include the lack of:

- A consistent methodology to cross-walk DHS-wide competencies;
- An effective process to analyze and identify cross-occupational competencies that lend themselves to the successful transitioning from one occupation to another; and,
- Tools and processes designed to effectively and consistently measure program activity and success.

**Question:** What is the leadership of the Department doing today, or intending to do in the near-term, to increase career mobility within the Department?

**Response:** The DHS Career Paths Program focuses on facilitating the movement of DHS employees between occupational groups, with a special emphasis on crossing Component lines. Currently, the Program focuses on certain law enforcement occupations, which lend themselves to cross-Component movement.<sup>1</sup> We have also identified three other occupations for inclusion in the Program. The Department plans to establish a cross-Component workgroup designed to examine the Career Paths Program and identify opportunities for expansion.

---

<sup>1</sup> For example, 1,664 DHS employees from other components were selected for Border Patrol and CBPO positions from 2007 to 2009.

<b>Question#:</b>	12
<b>Topic:</b>	career paths
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** How will the Department address any structural or long-term impediments to career mobility (as identified in the response to part 'a')?

**Response:** The Career Paths workgroup will continually evaluate and assess the program effectiveness; identify opportunities to enhance the Program; and develop effective strategies to address any identified impediments.

<b>Question#:</b>	13
<b>Topic:</b>	authority
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** When the Homeland Security Act of 2002 was originally enacted, it included a provision – section 872 – that allowed the Secretary broad authority to reorganize the Department, as long as the Secretary provided Congress with 60 days notice. The first two Secretaries of the Department made liberal use of this provision to combine, divide, create and move offices and functions within the Department. However, Congress, concerned that the Department was suffering from frequent and repeated reorganizations, has included in appropriations bills for the last number of years a provision prohibiting the Secretary from exercising her reorganization authority under section 872. The BUR lists as its first priority initiative to improve the Department's management the restoration of the Secretary's reorganization authority – at least with respect to DHS headquarters.

What is meant by the suggestion in the BUR that reauthorization authority is being requested only with respect to DHS headquarters? To which parts of the Department specifically would the Secretary's reorganization authority extend?

Only three other Department heads – the Secretary of Defense and, to a lesser extent, the Secretaries of Education and Energy – have any statutory reorganization authority beyond the implicit authority that all Cabinet Secretaries have to manage their departments. And none of these three has been given authority that approaches the breadth of that given to the Secretary of DHS under section 872. It may have made sense initially to include section 872 in the Homeland Security Act, as there would almost inevitably need to be some modifications to the structure of a Department that sought to integrate 22 different agencies. Why do you think it is still necessary, 7 ½ years after the Department was created, that the Secretary have such broad authority? Do you believe that the Secretary of Homeland Security should have broader reorganization authority than other Cabinet Secretaries, including the Secretary of Defense?

If section 872 authority is restored, what initial changes do you anticipate the Secretary making? In the absence of 872 authority, why has DHS not sought Congressional authorization directly for these changes?

**Response:** At its founding DHS was authorized to conduct reorganizations of Department functions upon 60 days notice to Congress, with the exception of USSS and USCG. Through subsequent appropriations language, this authority has been rescinded, and legislation such as the Post-Katrina Emergency Management Reform Act of 2006 has specifically added other DHS operational components (in that case, FEMA) to the

<b>Question#:</b>	13
<b>Topic:</b>	authority
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

original list of exempt organizations. DHS's proposal acknowledges that Section 872 authority is most appropriate for the Department's headquarters, as opposed to its operational components. However, it is imperative the Secretary have the flexibility to realign and restructure the Department's headquarters in the most efficient way to help align and unify departmental functions, especially as threats and challenges evolve over time. Section 872 authority does not obviate the need for notice and dialogue with Congress over DHS headquarters realignment and restructuring; however, it acknowledges that DHS's dynamic mission environment and continuing efforts to mature its Departmental operations require the Secretary to have the ability to evolve the Department headquarters structure to meet mission needs and drive forward Departmental maturity.

<b>Question#:</b>	14
<b>Topic:</b>	system
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** As the BUR notes, the primary vehicle for enhancing preparedness at the state and local level is the Department's homeland security grant programs, which provide almost \$4 billion annually to states, localities, first responders, and others. Both the Post-Katrina Emergency Management Reform Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act of 2007 include a number of provisions designed to ensure that these grant funds are spent effectively and are increasing state and national preparedness, including requirements for the development of performance metrics. GAO has estimated that from FY 2008 to FY 2010, FEMA budgeted roughly \$58 million to develop and implement several different evaluation efforts. Despite this, FEMA still cannot provide basic information on how these grants are being used or effectively measure how preparedness is increasing as a result. Recently, FEMA announced it was abandoning the development of its "Cost-to-Capabilities" system, the Department's latest effort to track and measure the capabilities being achieved through its homeland security grant programs.

Given the importance of these programs to state and local governments and first responders and the national need to better assess our preparedness, why did DHS decide not to include a performance measurement system for homeland security grant programs as a priority initiative or enhancement in the BUR? As an initiative not designated a priority, what resources and attention can we realistically expect DHS to devote to this effort?

**Response:** FEMA is committed to putting a system in place to measure State and local capacity and preparedness in an effective, coordinated manner by integrating existing assessment systems and considering grant effectiveness as part of the overall assessment of preparedness. A homeland security grant performance measurement system is an integral part of FEMA's preparedness assessment efforts.

Cost-to-Capabilities (C2C) was intended to be a tool to help grantees prioritize their investments and identify gaps in capability. Though the C2C project yielded valuable lessons learned, the pilot did not produce results that merited institutionalizing this particular approach. Lessons learned will be incorporated into FEMA's present efforts on assessment.

A review of the Department's efforts on State and local preparedness assessment revealed the existence of multiple federal assessment efforts. FEMA is integrating and improving



<b>Question#:</b>	14
<b>Topic:</b>	system
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

existing tools, like the State Preparedness Report, a web-based, streamlined, quantitative survey.

Before identifying a final assessment solution, FEMA is working to coordinate, integrate and streamline current efforts. FEMA has stood up a Congressionally-mandated Preparedness Task Force, which is comprised of Federal, State, Tribal, local, and private sector experts and charged with, among other duties, making recommendations as to the best system that should be implemented to measure national preparedness. Through the Task Force recommendations and better data collection and analytical products, FEMA will be able to deliver meaningful, useful, standards-based assessments of all-hazards preparedness.

Establishing a consolidated framework for the measurement of preparedness—that includes grant effectiveness—is a priority.

<b>Question#:</b>	15
<b>Topic:</b>	interoperability
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The QHSR notes that interoperability is a critical capability for first responders, and achieving interoperability for first responders is a major, unfinished recommendation of the 9/11 Commission. We have made some progress in bringing greater focus to the issue, including creation in the Post-Katrina Emergency Management Reform Act of the DHS Office of Emergency Communications, which has produced a National Emergency Communications Plan laying out broad goals for achieving interoperability and has helped States draft their own interoperability plans. But many obstacles remain, which relate partly to technical challenges but also to the need for better coordination at all levels of government on how to make different communications systems compatible. Unfortunately, there is reason to believe that if we had a Katrina-like disaster today, we would see many of the same communications problems we saw five years ago after Katrina.

Why did this issue not rank as something specific to mention in the BUR? What major initiatives is DHS undertaking right now to advance interoperability?

**Response:** Interoperable communications is referenced in the BUR as part of the DHS responsibilities for ensuring effective disaster response within the overall mission of Ensuring Resilience to Disasters. Several major initiatives are under way now to advance interoperability.

Established in 2007, the DHS Office of Emergency Communications (OEC) coordinates policy and assists in the development and implementation of interoperable and operable emergency communications capabilities for emergency responders at all levels of government—Federal, state, local, tribal, and territorial. OEC leads on a number of major DHS initiatives to advance interoperability and provides more than 100 technical assistance visits to state and local partners each year. These initiatives include:

- **National Emergency Communications Plan (NECP)**
  - Updating the NECP to address the use of broadband and other emerging technologies by first responders.
  - Evaluating NECP Goal 1, which states by the end of 2010, 90 percent of all high-risk urban areas designated within the Urban Areas Security Initiative (UASI) are able to demonstrate response-level emergency communications

<b>Question#:</b>	15
<b>Topic:</b>	interoperability
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

within one hour for routine events involving multiple jurisdictions and agencies.

- Planning to evaluate the compliance with NECP Goal 2 by 2011, which states that 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications in the event of a significant incident, as outlined in national planning scenarios, within three hours.

- **Emergency Communications Preparedness Center (ECPC)**

- Serving as the interagency focal point for coordinating Federal efforts to avoid unnecessary duplication and hindrances to emergency communications among the participating Federal Departments and Agencies.
- ECPC Focus Groups develop products to address legal and regulatory barriers and the coordination of grant administration.
- Continuing to coordinate interdepartmental efforts that drive implementation of the ECPC's Strategic Objectives, including development of capability mapping products.

- **The One DHS Emergency Communications Committee**

- Working towards the overall DHS Emergency Communications Strategy and initiation of governance and acquisition action plans across DHS.
- Focusing on the implementation of One DHS Emergency Communications Strategy actions, including consolidation of emergency communications investments across the Department and integration of voice, video and data capabilities.

- **Border Interoperability Demonstration Project (BIDP)**

- Awarding grants anticipated for September 2010 in coordination with DHS Management Directorate. These grants will be used for monitoring and project implementation as well as conducting technical assistance to the States awarded the grants.

- **Regional Coordinators**

- Coordinate and support Federal, state, local and tribal emergency communications activities, in addition to serving as liaisons to and from all of OEC.

<b>Question#:</b>	15
<b>Topic:</b>	interoperability
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

- OEC is developing roles and responsibilities for the Regional Coordinators.
- **SAFECOM** is a communications program of DHS. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, tribal, state, and Federal emergency response agencies.
  - Developed the Guidance for Federal Grant Programs, which provides consistent policy guidance on equipment, planning, and training standards.
  - Continues to share information by convening meetings for the Executive Committee, Emergency Response Council, and the Statewide Interoperability Coordinator Council to share challenges and solutions and to support OEC's achievement of NECP Goals and Milestones.
  - Provided Statewide Communication Interoperability Plan (SCIP) workshops to the states and territories to help them move towards fulfilling goals set forth in the NECP.

<b>Question#:</b>	16
<b>Topic:</b>	IA
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** One key enhancement identified by the BUR is expanding the Department's ability to provide security assistance and training for our international partners abroad. This issue has been especially important with the government of Mexico, which is courageously fighting the narco-terrorist cartels and which needs all the assistance we can provide. This Committee has held a series of hearings analyzing this conflict and our government's efforts to secure the border. And I must say that I was surprised to learn that DHS is unable to provide direct training for Mexico's border authorities without going through the State Department, a cumbersome process that takes a long time and is costly. While the Committee is encouraged by the BUR's commitment to expanding DHS' ability to provide international assistance, we are concerned that the Department did not request legislation to allow it to provide this kind of assistance directly to our foreign partners.

Do you believe that this kind of legislation would be useful for the Department and would help us better prepare our foreign partners for the all-too real security threats that they are facing?

**Response:** As noted in the Quadrennial Homeland Security Review, the Department's responsibilities "[require] international engagement." Indeed, international engagement and partnership is a priority for DHS and a key part of the Homeland Security enterprise. DHS continues to work closely with the Departments of State and Defense to use their foreign assistance authorities to provide, within the limits of their budgetary resources, assistance to our international partners. This includes specifically providing training for Mexican officials and officers through the Merida Initiative and Narcotics Affairs Section, among other sources, and advising DOS on the procurement of homeland security-related technology purchases. DHS looks forward to continuing and expanding—in collaboration with DOS and DOD—our international engagement.

<b>Question#:</b>	17
<b>Topic:</b>	distinctions
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The BUR and the QHSR draw distinctions drawn between activities within DHS that aim to prevent terrorism and those that aim to secure our borders. The Committee is somewhat concerned that this distinction may be overly simplistic. For example, according to the BUR the TSA is aligned with preventing terrorism and enhancing security, while CBP is aligned with border security. The recent attempted attacks on Christmas Day and on Times Square have shown that these distinctions are entirely non-existent. It was CBP, after all, that apprehended Faisal Shazhad as he tried to flee the United States. And CBP had identified that Umar Farouk Abdulmutallab warranted additional screening as he was in the air bound for Detroit.

Can you explain what exactly the distinction is at DHS between preventing terrorism and securing the border?

In the aftermath of the Christmas Day attempted attack, there were some indications that TSA and CBP were not on the same page when it came to the pre-screening of international travelers bound for the United States. The BUR and the QHSR's distinction between preventing terrorism and securing the border may undermine these agencies' ability to effectively work together to prevent terrorists from entering the country. Can you explain what DHS is doing to ensure that this is not occurring?

**Response:** Counterterrorism cuts across all of the homeland security missions. Homeland security relies on our shared efforts to prevent and deter attacks by identifying and interdicting threats, denying hostile actors the ability to operate within our borders, and protecting the Nation's critical infrastructure and key resources. A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders; that we safeguard lawful trade and travel; and that we disrupt transnational organizations that engage in smuggling and trafficking across the U.S. border. Both CBP and TSA prevent terrorism as a result of successfully executing these functions, in addition to engaging in specific activities aimed at countering terrorism.

Effectively controlling U.S. air, land, and sea borders is just one of many objectives that support preventing terrorist attacks. Others include:

- Managing risks to critical infrastructure, key leadership, and events;
- Safeguarding lawful trade and travel;
- Preventing unlawful immigration;
- Creating a safe, secure, and resilient cyber environment; and

<b>Question#:</b>	17
<b>Topic:</b>	distinctions
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

- Ensuring the protection of privacy, civil rights and civil liberties.

Our borders are not our first line of defense against global threats; they are an integral part of any strategy to counter terrorism as key nodes in global systems that carry people, goods and data around the world. These systems underpin a strong and competitive U.S. economy, but are also vulnerable to exploitation by our adversaries, terrorists, and criminals. We must work to confront this exploitation at every opportunity along the supply chain, including border crossings and aviation security checkpoints. Security and expediting and enforcing lawful trade, travel, and immigration are mutually reinforcing and inextricably intertwined through actions such as screening, authenticating, and maintaining awareness of the flow of people, goods, and information around the world and across our borders.

Ensuring that DHS Operational and Support Components are coordinating towards all of the QHSR Mission areas (including preventing terrorism and securing our borders) requires planning at all levels.

<b>Question#:</b>	18
<b>Topic:</b>	travel
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Committee was encouraged by the QHSR's focus on looking "beyond our borders to identify and disrupt threats well before they reach our shores," and its emphasis on working with our international partners to enhance the security agreements that are in place to prevent terrorists from traveling. It is vital to our homeland security for DHS to have access to the specific identifying information that it needs to match individuals on the terrorist watch list to passenger manifests well before those individuals reach the airport.

Although the BUR includes a goal of strengthening aviation security, it focuses more on physical screening and does not mention the importance of international agreements that was a focus of the QHSR. Can you explain in the context of the BUR how the Department will be working to enhance our ability to pre-screen international travelers bound for the United States?

**Response:** DHS, including U.S. Customs and Border Protection (CBP), administers a number of overlapping programs designed to screen international travelers bound for the United States in advance of arrival.

US Customs and Border Protection (CBP) administers the Immigration Advisory Program (IAP), which is a partnership between CBP, foreign governments, and commercial air carriers to identify and prevent high-risk and improperly documented travelers from boarding US-bound flights. IAP is operational in ten locations in eight countries: Amsterdam, Frankfurt, Incheon (Seoul), London (Heathrow and Gatwick), Madrid, Manchester (UK), Narita (Tokyo), Paris, and Warsaw.

IAP teams have excellent relationships with host country authorities, allowing them to receive information regarding local trends in fraudulent document and mala fide traveler intercepts. CBP officers working on IAP teams are able to intercept and coordinate with foreign authorities to prevent a passenger from boarding a flight when the passenger presents a security concern, is attempting to travel on fraudulent documents, or is likely to be found inadmissible on arrival in the U.S. Privileged access to the airside passenger areas of the airports enables IAP to provide an unprecedented level of support to air carriers, host governments, U.S. embassies, and DHS Attachés. Furthermore, as CBP continues to hone its scenario- and intelligence-based targeting rules, previously unknown individuals identified by these rules will be referred to IAP locations. Officers



<b>Question#:</b>	18
<b>Topic:</b>	travel
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

on-site can then assess the perceived threat posed by such individuals and work with foreign authorities and carriers to take the appropriate action.

Additionally, CBP works closely with Mexican Authorities through the Joint Security Program to identify high risk travelers. CBP officers on site at the Mexico City airport work in conjunction with Mexico Immigration, Federal Police and Intelligence Agencies on identifying travelers who do not possess the proper documentation to enter or transit the United States or Mexico, or who may otherwise be inadmissible upon arrival in the United States or Mexico.

On January 10, 2010, CBP also began pre-screening passengers traveling from non-IAP locations. To accomplish this goal, the National Targeting Center, Passenger (NTC-P) works in coordination with CBP officers assigned to the Regional Carrier Liaison Groups (RCLG) who are CBP's regional points of contact and coordination between international carriers, foreign immigration authorities and other DHS entities. CBP officers at the NTC-P work with the RCLG officers to make recommendations to carriers in foreign locations that boarding be denied (off-loads) to individuals traveling to the United States who have been identified as being national security related threats, ineligible for admission or who are traveling on fraudulent or fraudulently obtained documents prior to boarding a flight to the United States. CBP also coordinates with ICE Attaches and Legal Attaches and Air Carrier Security Offices on high risk passengers.

CBP's Preclearance program is another program in which CBP partners with foreign governments and commercial air carriers to pre-inspect travelers and includes the full range of vetting and screening that occurs at any U.S. port of entry, except it is conducted on foreign territory. In most instances, a foreign government requests consideration of initiating preclearance operations. In response to a request, the Department of Homeland Security (DHS), in collaboration with the relevant component agency, conducts a thorough review of the proposal to determine feasibility of meeting established operational requirements prior to entering into exploratory discussions with the host government; which may lead to negotiation of a Preclearance agreement between the U.S. government and the foreign government to initiate preclearance operations once requirements are met. The agreements vary by country and these agreements are often classified.

CBP is mindful of the significant resource implications associated with preclearance operations; and at this time is not looking to further expand the preclearance program. Section 711 of the "Implementing the Recommendations of the 9/11 Commission Act of 2007" (P.L. 110-53; 9/11 Act) created mechanisms to expand membership and enhance

<b>Question#:</b>	18
<b>Topic:</b>	travel
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

the security of the Visa Waiver Program (VWP). In response to this requirement, CBP, in consultation with the Department of State (DOS), developed Electronic System for Travel Authorization (ESTA) program to collect and screen biographic information and responses to VWP eligibility questions from VWP citizens or nationals to determine their eligibility to travel to the United States under the VWP. The development and implementation of ESTA represents a major change in visa-free travel to the United States. CBP, in coordination with other U.S. Government partners, has made great strides in communicating the ESTA requirement to VWP stakeholders. CBP remains committed to continuing to work with the VWP traveling public, air and sea carriers, and the travel industry to further ensure stakeholder buy-in and commitment and to facilitate 100-percent compliance with the ESTA requirement.

DHS continues to work with interested foreign governments on collaborative arrangements; the purpose of these efforts is to identify higher-risk travelers intending to travel to the United States prior to their actual departure from overseas locations.

<b>Question#:</b>	19
<b>Topic:</b>	CIS
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The BUR highlights the need for enhanced catastrophic disaster preparedness and emphasizes that planning assumptions must address worst case scenarios. The need for catastrophic planning has never been clearer as we approach the five year anniversary of Hurricane Katrina and as we watch the Gulf Coast struggle again – this time to recuperate from the catastrophic Deepwater Horizon oil spill. While it was good to see catastrophic disaster preparedness included in the BUR, there was little description of this initiative in the BUR. For instance, DHS still has not completed revising the Catastrophic Incident Supplement – an action required by the Post-Katrina Act passed into law in October 2006. The failure to complete this essential plan puts the nation at great risk.

When will the Department finalize an updated Catastrophic Incident Supplement? Given that the Catastrophic Incident Supplement was not mentioned in the BUR, is completion of the revised Catastrophic Incident Supplement a priority for DHS?

**Response:** The Catastrophic Incident Supplement (CIS) has not been updated. The revision to the CIS was placed on hold because of the rewrite of HSPD-8 and the ultimate replacement of HSPD-8 with the soon to be issued White House Presidential Policy Directive (PPD) on National Preparedness. Because the new PPD on National Preparedness will have such a significant impact on future planning activities, the decision was made to place on hold any further revision to the CIS. Once the new National Preparedness PPD is issued, a determination will be made on whether the CIS will ultimately be revised as a stand-alone document or incorporated into the larger planning effort that will be required by the new PPD. The new PPD incorporates the framework of mitigation with the prevention, protection, response and recovery frameworks.

At the same time, FEMA is also undertaking a “Whole Community Catastrophic Response” initiative as one of the Administrator’s strategic priorities. This initiative will focus on critical disaster response operations needed in the first 72-hours following an extreme disaster that overwhelms the existing federal-state-local emergency support capacity. The results of this initiative will also be used in addition to the new PPD to help inform future decisions on the best course of action for revising the CIS or incorporating it into the new planning efforts.

<b>Question#:</b>	20
<b>Topic:</b>	FEMA
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** When DHS released the QHSR, we were told by DHS that more details were coming in the format of a bottom-up-review, the BUR. But now that the BUR has been released, many are still wondering where the details are, particularly with regard to improving the nation's resiliency to disasters. While the QHSR recognizes that FEMA must continue to make strides in its capabilities, the BUR doesn't go far enough in providing details on how the department will accomplish this. The Post-Katrina Emergency Management Reform Act authored by Senator Collins and myself creates a new FEMA with missions and authorities far exceeding the old FEMA. Complete implementation of the Post-Katrina Act is something that will still require sharply focused initiatives and hard work.

Can you provide more specifics of FEMA initiatives for the next few years that will ensure complete implementation of the Post-Katrina Act?

**Response:** FEMA remains committed to continuing to implement the provisions of the Post-Katrina Emergency Management Reform Act (PKEMRA) and to ensuring the authorities and flexibilities in the law are implemented as well. Substantial progress has already been made, and several of the outstanding deliverables are nearing completion. The following are some examples of FEMA's progress and plans moving forward to complete implementation of PKEMRA.

National Advisory Council – FEMA has greatly benefitted from the establishment of the National Advisory Council, which provides valuable advice on a number of initiatives early in the concept development phase, in order to solicit feedback and gain stakeholder buy-in before initiatives are completed. The NAC is comprised of a diverse group of emergency management leaders and partners.

National Disaster Housing Strategy – PKEMRA mandated that FEMA create the National Disaster Housing Strategy (Strategy). The Strategy, published in January 2009, calls for the establishment of a National Disaster Housing Task Force (NDHTF) to provide a full-time, multi-agency focus on disaster housing related issues, to elevate the significance of disaster housing preparedness in all jurisdictions, and to oversee implementation of the Strategy.

The NDHTF, staffed and led by FEMA, is made up of multiple key Federal agency partners including DHS, DOJ, DOI, EPA, GSA, HHS, HUD, NCD, SBA, USACE,

<b>Question#:</b>	20
<b>Topic:</b>	FEMA
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

USDA, VA and the U.S. Access Board. The NDHTF developed an Implementation Plan for the Strategy which describes how members of the Task Force will move toward connecting critical programs with interagency, intergovernmental, and non-governmental organizational efforts in order to accomplish the goals of the Strategy, and will help to ensure that the Strategy is effectively incorporated into existing emergency plans, procedures, and policies by providing measurable objectives, specific actions, and achievable milestones. Additionally, the NDHTF facilitates interagency disaster housing planning efforts, encourages preparedness and planning activities by State and local governments, private sector and non-governmental agencies.

The NDHTF is currently focused on finalizing a disaster housing Concept of Operations (CONOPS) and a Disaster Housing Practitioners' Guide through a collaborative process among the various local, State, tribal and Federal partners, nongovernmental organizations, and the private sector to meet the needs of all disaster survivors. The CONOPS lays out how the range of Federal agencies involved in disaster housing coordinate response efforts and explains the Federal Government's housing support role to State and local partners in operational terms for the normal range of disasters, along with the responsibility to maintain readiness to assume a greater role in housing disaster survivors in response to catastrophic events. Additionally, the CONOPS will convey national guidance, operating principles, and a vision for public (Federal, state, tribal, local), private, and non-profit cooperation in providing disaster housing assistance. It defines the roles, programs, authorities, and responsibilities of all entities, detailing shared responsibilities and emphasizing the cooperative efforts required to provide disaster housing assistance.

The Practitioners' Guide will serve as a guide for State, local, tribal, and territory disaster housing assistance practitioners to establish their own State-Led Disaster Housing Task Forces and to develop disaster housing strategies that improve disaster responsiveness and consider the unique needs of all people displaced by disasters. The Practitioner's Guide will provide tools for individual entities, such as the State-Led Disaster Housing Task Forces, and local governments to operate or to create housing plans. The Practitioners' Guide also identifies preparedness and mitigation measures that enable State, local, tribal, and territory governments to better prepare for, respond to, and recover from different types and levels of disasters and resulting housing needs.

To ensure consistency, the completion of the NDHTF's CONOPS, Charter, and the Disaster Housing Practitioners' Guide are set to coincide with the release of the National Disaster Recovery Framework (NDRF).

<b>Question#:</b>	20
<b>Topic:</b>	FEMA
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

Following development of these guiding documents, the NDHTF will shift focus to seeking improvements in the delivery of disaster housing assistance, and ensuring coordination between partners to improve the entire continuum of disaster housing, from sheltering to permanent housing.

Reducing Waste, Fraud, and Abuse – PKEMRA created several provisions in order to prevent waste, fraud and abuse in the contracting and relief aid processes. To this end, FEMA implemented new software in 2007, communicating real-time data to caseworkers in order to prevent duplicate housing payments. FEMA also implemented checks in the National Emergency Management Information System (NEMIS) that trigger additional review for 'high risk' recipients before assistance is delivered, in order to prevent potential fraud. These actions allow FEMA to balance the need to quickly provide disaster aid to victims with our responsibility to be good stewards of the Disaster Relief Fund, ensuring that federal funds are used properly.

National Emergency Family Register and Locator System – FEMA has established a national emergency family register and locator system and a national emergency child locator center to help displaced persons find their loved ones. FEMA has worked with its partners to provide basic life support, first aid, and education, as well as all-hazards preparedness training to children in grades one through seven, caregivers, parents, and responders. The agency also supports team community emergency response training for high school students. Additionally, FEMA has placed significant focus on planning for all members of affected communities, including infants, children, and the disabled.

Private Sector Integration – PKEMRA has helped FEMA to integrate the private sector into preparedness, response and recovery efforts. In 2007, FEMA established a Private Sector Division of External Affairs, in response to recommendations in PKEMRA. FEMA's Private Sector Division facilitates full engagement of the private sector – including business and industry, academia, non-profit and other non-governmental organizations – as a key player in disaster preparedness, response and recovery.

Comprehensive Preparedness System – In terms of Subtitle C of PKEMRA, Comprehensive Preparedness System, the new Presidential Preparedness Directive (PPD) on National Preparedness, FEMA is involved with an interagency group that is drafting an updated PPD that is anticipated to address the call for an update of the National Preparedness Goal (PKEMRA Section 643). Since the formal implementation of the NPG in September 2007, FEMA's understanding of the nation's risks and capabilities has evolved, and national preparedness concepts, policy, doctrine, and target capabilities have matured. Once the PPD is finalized and signed, FEMA is expected to conduct a

<b>Question#:</b>	20
<b>Topic:</b>	FEMA
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

comprehensive review, update the NPG, and develop a schedule to identify and synchronize major preparedness program activities, a clear delineation of roles and responsibilities, and specific supporting courses of action across each element of the preparedness cycle (i.e. plan, organize and equip, train, exercise, evaluate, and improve). This update will describe the process for incorporating developments in policy, doctrine, and lessons learned into preparedness activities, as well as how exercises, evaluations, and assessments evaluate risks, capabilities, and needs to advance national preparedness.

Finally, PKEMRA enabled FEMA to strengthen its partnerships within the entire emergency management community through the establishment of a small state and rural advocate and a national disability coordinator. The national disability coordinator's office has subsequently been expanded to an Office of Disability Integration and Coordination.

While completing implementation specific actions mandated by PKEMRA is a priority, we also must continuously work to ensure that our policies are consistent with the PKEMRA, and maximize the tools available to us under the FEMA's authorities in order to effectively respond to the needs of individuals and states following a major disaster. FEMA recently completed an aggressive review of all disaster assistance policies in the Individual Assistance (IA) and Public Assistance (PA) Divisions apart from the three-year cyclical review. In addition to these efforts, the National Advisory Council has placed priority on identifying areas where changes in the PKEMRA-implementing regulations and policy can most quickly and directly result in greater flexibility in providing assistance.

The QHSR and the Bottom Up Review report complement PKEMRA and provide a framework for FEMA's efforts to "Ensure Resilience to Disasters." The following provides additional information regarding FEMA BUR initiatives that are consistent with PKEMRA and will help build national resilience.

BUR Initiative #29: Enhance Catastrophic Disaster Preparedness.

The FEMA Administrator has directed FEMA staff to first define and then implement a "whole of community" focused preparedness and response national-level capacity to improve our resilience to extreme disasters, and enhance our ability to save and sustain lives following a catastrophic event, with the additional goal of stabilizing the event within 72 hours. By the start of FY 2012, FEMA expects to have developed key doctrine and procedures and prioritized disaster outcomes for each representative catastrophic meta-scenario. The focus of FY 2012, efforts will be on implementation of this initiative, in coordination with "whole of community" partners, through training, planning projects,

<b>Question#:</b>	20
<b>Topic:</b>	FEMA
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

exercises, and supporting policies and documents (e.g., pre-scripted mission assignments). For example, one significant current planning effort is the formulation of a plan to address a catastrophic earthquake impacting eight states in the New Madrid Seismic Zone. This initiative integrates plans at all levels of government with an overarching national-level earthquake plan and provides the basis for a fundamental re-tooling of all-hazards catastrophic incident guidance. The experience from this planning effort is being applied to other key planning activities.

BUR Initiative #30: Improve DHS' ability to lead in emergency management.

FEMA is exploring opportunities to improve the lifecycle of FEMA's workforce, from recruitment through professional growth into the most senior levels of leadership. The core objective is to create an improved work environment for FEMA's current and future employees, including interns. The objective will be substantially achieved through enhanced recruitment, hiring, and developmental initiatives and opportunities. In FY 2012 FEMA will complete strategic workforce planning efforts and present implementation strategies to support development of both FEMA's workforce and across the entire field of emergency management. Leadership will then be able to make decisions regarding any future resource implications and begin to implement resource neutral options as appropriate.

BUR Initiative #32: Make individual and family preparedness and critical facility resilience inherent in community preparedness.

Numerous offices and divisions within FEMA and DHS have initiatives and programs that support this goal through technical and social science research, partnerships with government and civic organizations at all levels, and tools and resources for state, tribal, local, family and individual execution. In addition, the proposed new Presidential Policy Directive (PPD) on National Preparedness is expected to require DHS and FEMA to develop a national strategy that promotes and enables "whole of community" participation and involvement in national preparedness. This strategy should be completed by the start of FY 2012 and include five components: National Leadership Voice and Collaborative Partnerships; Doctrine, Policy, Strategic Planning; Public Outreach and Training; Tools and Resources for local implementation; Evaluation and Recognition of Success. The focus of FY 2012 efforts will be on continued implementation of these strategies and expanded use of the Citizen Corps and Ready.Gov programs.



<b>Question#:</b>	21
<b>Topic:</b>	private sector
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Implementing Recommendations of the 9/11 Commission Act of 2007 required DHS to implement a voluntary program to certify the preparedness of private sector companies not later than 210 days after enactment. Unfortunately, the previous Administration missed the statutory deadline for implementation and failed to widely promote the program. To date the program still has not been implemented, nor has it been promoted as required by the law. Although I was pleased that this program was mentioned in the BUR and pleased that the Department recently announced the standards that will be used for the program, the Department's failure to completely implement the program is regrettable. Given that the private sector controls 85 percent of the critical infrastructure in the Nation, the importance of enhancing private sector preparedness cannot be understated. The 9/11 Commission found that the private sector remains largely unprepared for disasters, and the recent devastating oil spill in the Gulf of Mexico serves as a painful reminder of why private sector preparedness is so important.

When will DHS have the program fully implemented? Please describe your plan for the future promotion of this program.

**Response:** DHS will begin an aggressive campaign to raise awareness of the PS-Prep Program and how private sector organizations can participate to coincide with National Preparedness Month in September 2010. DHS plans to roll-out a small business-specific certification initiative in the fall of 2010.

## Private Sector Preparedness in the DHS QHSR

PS-Prep is recommending the following performance measures to be added to the DHS QHSR missions, goals, and objectives that are specific to private sector preparedness.

### I. Recommended Private Sector Preparedness Outcome Measures

We recommend outcome measures specific to private sector preparedness for the following goals and objectives under Mission 5: Ensuring Resilience to Disasters.<sup>1</sup>

#### Goal 5.4: Rapidly Recover

- Objective 5.4.1: Enhance recovery capabilities
- Objective 5.4.2: Ensure continuity of essential services and functions

##### Outcome Measures (Applicable for Goals 5.1 and 5.4):

- Developing measures on level of voluntary nationwide participation in Private Sector Preparedness Accreditation and Certification Program (PS-Prep). One element of Accreditation will be a business continuity plan.

#### Goal 5.2: Enhance Preparedness

- Objective 5.2.2: Strengthen capabilities

##### Outcome Measures:

- Percent of private sector organizations that are engaged in preparedness activities such as education and training, organizational development, and or assessment.
- Percent of private sector organizations reporting they are or plan to formally **certify to** one or more DHS adopted preparedness standards through the PS-Prep Program.
- Percent of private sector organizations reporting they are utilizing one or more DHS adopted preparedness standards outside of the formal PS-Prep Program conformity assessment processes.
  - Percent of private sector organizations reporting their known or desired impact on community, individuals, business operations, or supply chain based on the formal PS-Prep Program conformity assessment activities in which they are engaged.

<sup>1</sup> There are five missions outlined in the QHSR: Mission 1- Preventing Terrorism and Enhancing Security, Mission 2- Securing and Managing Our Borders, Mission 3- Enforcing and Administering Our Immigration Laws, Mission 4- Safeguarding and Securing Cyberspace, and Mission 5- Ensuring Resilience to Disasters.

**Goal 5.3: Ensure Effective Emergency Response**

- Objective 5.3.1: Provide timely and accurate information to the public
- Objective 5.3.2: Conduct effective disaster response operations
- Objective 5.3.3: Provide timely and appropriate disaster assistance

**Outcome Measures:**

- Percent of private sector organizations that have public crisis communications plan.
- Percent of private sector organizations that have trained relevant staff to the public crisis communication plan.
- Percent of private sector organizations reporting they have or plan to exercise their business continuity plan in coordination with local/state officials, supply chain, and other applicable public and private sector partners.
- Percent of private sector organizations reporting that they have or plan to utilize lessons learned and after action report outcomes to update and enhance their business continuity plan.

<b>Question#:</b>	22
<b>Topic:</b>	HSAS
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Joseph I. Lieberman
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** In September 2009 a Task Force of the Homeland Security Advisory Council completed a review of the Homeland Security Advisory System (HSAS) that had been requested by the Secretary in July 2009. Since the completion of that review, no changes have been made (at least publicly) to the HSAS.

What is the status of efforts to modify the Homeland Security Advisory System following the September 2009 HSAC review? Have any changes been made to the HSAS since September 2009?

**Response:** The task force helped to develop actionable recommendations regarding potential changes to the Homeland Security Advisory System. The recommendations and any potential changes to the system are currently being discussed in the interagency process.

**Post-Hearing Questions for the Record  
Submitted to the Honorable Jane Holl Lute  
From Senator Claire McCaskill**

***“Charting a Path Forward: The Homeland Security Department’s Quadrennial  
Homeland Security Review and Bottom-Up Review”  
July 21, 2010***

<b>Question#:</b>	23
<b>Topic:</b>	PMO
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** One of the 44 initiatives identified in the Bottom-Up Review (BUR) is to reduce DHS’ reliance on contractors, and I understand that DHS is creating a specific Program Management Office (PMO) to handle a Workforce Balance assessment, but I am concerned about the timeliness of these initiatives. For example, in December 2009, DHS stated that 3,500 contractor positions had been identified as being more appropriate for performance by Federal employees and that conversions would take place by the end of FY10, but in April 2010 DHS stated that these conversions may carry over into FY2011. Then in May 2010, DHS stated that there were delays and favorable miscalculations, and now the Department estimates that 700 of these positions will be on board by the end of FY10. There are thousands of contractors that this PMO will potentially identify for conversion in the near future. What will DHS do to ensure a more efficient and effective process? Can Congress do anything to enable a more efficient conversion process? Please explain.

**Response:** The initial effort to address potential contractor over-reliance was based on a March 2009 data call that asked components to identifying contracts that potentially included “inherently governmental” or “closely associated with inherently governmental” work. This data call, and the components’ responses, took place prior to OMB’s issuance of the Memorandum on the Multi-sector Workforce, which provided direction to executive agencies on determining the proper balance between federal and contractor workforces.

As a result of the March 2009 data call, the then Under Secretary for Management approved the conversion to Federal service of 3,500 positions. As insourcing progressed, the Department learned numerous lessons, including the need for:

- More comprehensive guidance to the components;
- Greater standardization of processes and documentation of decisions;

<b>Question#:</b>	23
<b>Topic:</b>	PMO
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

- Increased, habitual senior-level attention, particularly at the component level;
- Regularly scheduled, consistent reporting on progress and results;
- Clearly defined outcomes; and
- Shift in primary focus on the number of contractor positions eliminated; as opposed to a one for one conversion from contractor to federal positions. This became evident as a result of an analysis which revealed the work of some contractor positions was absorbed by existing Federal employees and multiple part-time contractor positions were filled via full-time federal employment.

The Balanced Workforce Program Management Office was established in March 2010 and has since accomplished the following:

- Issued preliminary Balanced Workforce Strategy Guidance on July 13, 2010, and final Guidance on August 2, 2010, which outlines a 3-step process to determine the appropriate workforce mix, and includes detailed instructions;
- Conducted a day-long training event for Department level senior executives on the Balanced Workforce Strategy on July 13, 2010;
- Organized and held the first meeting of the Balanced Workforce Executive Steering Group composed of a senior executive component representatives on August 3, 2010;
- Deployed an intranet web site to provide background materials and guidance information for use by components as they implement the Balanced Workforce Strategy;
- Developed a methodology for prioritizing service contracts and issued a timetable for contract review to members of the Executive Steering Group; and
- Designed a survey tool, currently undergoing in-depth technology testing, to serve as the "repeatable process" to conduct the analysis of federal and contractor work.

The process to analyze and make determinations of the proper workforce balance has been developed. We will gauge the implementation effort as we go forward, which will enable us to notify the Congress if specific assistance is needed.

<b>Question#:</b>	24
<b>Topic:</b>	conversions
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The DHS/Chief Human Capital Officer (CHCO) also mentioned as part of their response of why so few positions are planned to be converted by the end of FY2010 was because “some of the functions and activities previously performed by contractors were absorbed by existing Federal employees, a result not anticipated by the Components when they identified the 3,500 positions.” How many of these positions were absorbed by existing Federal employees? Does DHS plan to track the cost savings realized from this review and conversion process? What does DHS plan to do with the cost savings once identified?

**Response:** As of August 14, 2010, of the 3,500 contractor positions identified for conversion, a total of 1,596 have been eliminated. As a result, a total of 1,323 new Federal positions have been established from dollars formerly dedicated to contracts of which 843 of those positions have been filled with Federal employees. As part of this initiative, the workload that was previously performed by contractors that may have been absorbed by existing Federal employees has not been recorded.

The Department will detail the cost savings from converting and eliminating contractor positions in the Congressional Budget Justification.

Once identified, the Department intends to use conversion-related savings to fund other areas of the Department critical to our mission.

<b>Question#:</b>	25
<b>Topic:</b>	breakout
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Chief Human Capital Officer (CHCO) stated that it will cost \$1.38 million (salaries, benefits, and shared services) in FY11 for six resources; one Senior Executive Service (SES), one GS-15, and four Full Time Equivalents (FTEs) for this new PMO dedicated to determining the optimum federal employee-to-contractor ratio. CHCO stated that the FY11 Budget request alone for the four FTEs was \$900,000. Are these positions going to be mid-grade level federal employees since an SES and a GS-15 are being paid for out of existing baseline funds? If so, why does a mid-level federal employee cost an average of \$225,000? Please provide a breakout per employee of this \$900,000 cost estimate.

**Response:** The FY 2011 budget request for the Office of the Chief Human Capital Officer PPA requested 108 FTP/FTEs and \$24.999 million which includes \$900,000 to support the Balanced Workforce Strategy. The \$900,000 supports the salaries, benefits, expenses and Working Capital Fund shared services of three GS-14 positions, one GS-13 position and minimal funding for contractor support to assist the program office during the first quarter of the fiscal year. A breakout of the \$900,000 is provided below:

Salaries and benefits for (3) GS-14s (assumes a step 5 and 1.4% pay inflation)	\$464,283
Salaries and benefits for (1) GS-13 (assumes a step 5 and 1.4% pay inflation)	\$130,965
WCF Shared Services (4 positions)	\$180,000
Expenses (travel, training, supplies, awards, etc)	\$31,000
Contractor Support (1st quarter FY 2011)	\$93,700
<b>Total</b>	<b>\$899,948</b>



VerDate Nov 24 2008 10:14 Nov 08, 2011 Jkt 58402 PO 00000 Frm 00093 Fmt 06601 Sfmt 06601 P:\DOCS\58402.TXT SAFFAIRS PsN: PAT

<b>Question#:</b>	26
<b>Topic:</b>	timeframe
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Office of Chief of Human Capital Officer (CHCO) stated that in the near term, the balanced workforce strategy will address pressing issues related to the appropriate balance of federal staff to contractors, and over time, the balanced workforce strategy will evolve into the department's overall workforce planning model. What is the timeframe for determining the optimum federal government-to-contractor ratio? What are the specific plans for this PMO after this optimum federal staff to contractor's ratio level is achieved?

**Response:** At this time, we do not anticipate that the Balanced Workforce Strategy will produce an overall "optimum federal staff to contractor ratio." It is possible that, as work is analyzed, an "optimum federal staff to contractor ratio" may be an output of the Balanced Workforce Strategy process. However, as currently structured, not every service contract can be quantified as consisting of a specific number of contractor positions. We would need that information in order to create a ratio.

A full-scale Balanced Workforce review of contracts and federal work will take approximately three fiscal years. Our initial focus is on high priority service contracts. We will then expand the analysis to all aspects of DHS work. As DHS components, managers, and business support organizations gain more experience with the Balanced Workforce process, we expect to move more quickly in conducting the analyses and then implementing any needed adjustments to the workforce balance.

Once the initial round of analysis is completed, the PMO will be needed to update policy, guidance, and processes on a regular basis, and also provide oversight and reporting on the workforce. We also anticipate that additional workforce planning actions, such as designation of mission critical occupations and identification of needed competencies and skills will be incorporated logically into the PMO. The PMO has already begun work on revising the DHS Workforce Planning Guide to incorporate the Balanced Workforce Strategy guidance.

<b>Question#:</b>	27
<b>Topic:</b>	detail
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** The Chief Human Capital Officer (CHCO) recently provided me a breakdown of the FY09 support service contractors from the Federal Procurement Data System (FPDS). It showed ~\$10.97 billion was executed on service support contractors and over 33% (~\$3.68 billion) of this was executed on professional, administrative, and management support services. The next two categories were IT-related support at \$2.22 billion (~20%) and Utilities and Housekeeping at \$1.51 billion (~14%). This \$3.68 billion does not include research and development support, architecture/engineering services, education/training services, medical services, maintenance/building repair, or quality control, test and inspection support services. Please explain a little further what these professional, administrative, and management support services are being used for that costs \$3.68 billion?

**Response:** The Chief Procurement Officer (CPO) indicated that the \$3.68 billion includes the following services:

<b>FY09 Professional Services (R SERVICES (other than Research and Development))</b>		
<b>PSC Code (Description)</b>	<b>Total Dollars</b>	<b>% Total Dollars</b>
R499 (OTHER PROFESSIONAL SERVICES)	\$880,666,544.41	23.8865%
R408 (PROGRAM MANAGEMENT/SUPPORT SERVICES)	\$875,390,243.57	23.7434%
R425 (ENGINEERING AND TECHNICAL SERVICES)	\$568,805,915.68	15.4279%
R799 (OTHER MANAGEMENT SUPPORT SERVICES)	\$435,411,412.54	11.8098%
R414 (SYSTEMS ENGINEERING SERVICES)	\$148,716,488.48	4.0337%
R699 (OTHER ADMINISTRATIVE SUPPORT SVCS)	\$140,795,464.89	3.8188%
R421 (TECHNICAL ASSISTANCE)	\$70,656,305.61	1.9164%
R426 (COMMUNICATIONS SERVICES)	\$64,976,961.37	1.7624%
R710 (FINANCIAL SERVICES)	\$62,002,813.35	1.6817%
R707 (MGT SVCS/CONTRACT & PROCUREMENT SUP)	\$56,305,776.82	1.5272%
R706 (LOGISTICS SUPPORT SERVICES)	\$46,940,225.13	1.2732%
R701 (ADVERTISING SERVICES)	\$46,244,296.25	1.2543%

<b>Question#:</b>	27
<b>Topic:</b>	detail
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

R419 (EDUCATIONAL SERVICES)	\$36,476,747.91	0.9894%
R703 (ACCOUNTING SERVICES)	\$27,269,410.86	0.7396%
R402 (REAL ESTATE BROKERAGE SERVICES)	\$26,395,992.23	0.7159%
R604 (MAILING AND DISTRIBUTION SERVICES)	\$26,021,642.95	0.7058%
R407 (PROGRAM EVALUATION SERVICES)	\$18,954,954.00	0.5141%
R603 (TRANSCRIPTION SERVICES)	\$17,270,326.70	0.4684%
R423 (INTELLIGENCE SERVICES)	\$15,944,916.00	0.4325%
R612 (INFORMATION RETRIEVAL)	\$14,533,987.54	0.3942%
R405 (OPERATIONS RESEARCH & QUANTITATIVE)	\$14,053,403.06	0.3812%
R409 (PROGRAM REVIEW/DEVELOPMENT SERVICES)	\$13,145,178.18	0.3565%
R608 (ADMIN SVCS/TRANSLATION-SIGN LANGUAG)	\$11,896,625.94	0.3227%
R708 (PUBLIC RELATIONS SERVICES)	\$8,700,442.02	0.2360%
R702 (DATA COLLECTION SERVICES)	\$6,861,477.58	0.1861%
R415 (PROF SVCS/TECH SHARING-UTIL)	\$5,920,881.95	0.1606%
R420 (CERTIFICATIONS & ACCREDIT PROD & IN)	\$5,101,879.73	0.1384%
R704 (AUDITING SERVICES)	\$5,085,692.80	0.1379%
R498 (PATENT AND TRADEMARK SERVICES)	\$4,520,919.93	0.1226%
R411 (PROF SVCS/REAL PROPERTY APPRAISALS)	\$4,230,466.17	0.1147%
R497 (PERSONAL SERVICES CONTRACTS)	\$3,840,672.62	0.1042%
R406 (POLICY REVIEW/DEVELOPMENT SERVICES)	\$3,728,316.00	0.1011%
R607 (WORD PROCESSING/TYPING SERVICES)	\$3,453,021.39	0.0937%
R418 (LEGAL SERVICES)	\$3,258,728.34	0.0884%
R416 (VETERINARY/ANIMAL CARE SERVICES)	\$3,001,149.62	0.0814%
R428 (INDUSTRIAL HYGIENICS)	\$2,411,621.12	0.0654%
R605 (LIBRARY SERVICES)	\$1,745,443.10	0.0473%
R611 (CREDIT REPORTING SERVICES)	\$1,524,906.10	0.0414%
R602 (COURIER AND MESSENGER)	\$1,387,892.09	0.0376%

<b>Question#:</b>	27
<b>Topic:</b>	detail
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

SERVICES)		
R709 (ONGOING AUDIT OPERATIONS SUPPORT)	\$1,182,517.64	0.0321%
R422 (MARKET RESEARCH & PUBLIC OPINION SE)	\$651,347.28	0.0177%
R412 (SIMULATION)	\$399,424.88	0.0108%
R614 (PAPER SHREDDING SERVICES)	\$310,347.00	0.0084%
R606 (COURT REPORTING SERVICES)	\$187,496.98	0.0051%
R413 (SPECIFICATIONS DEVELOPMENT SERVICES)	\$173,151.40	0.0047%
R711 (BANKING SERVICES)	\$154,162.76	0.0042%
R613 (POST OFFICE SERVICES)	\$54,449.79	0.0015%
R424 (EXPERT WITNESS)	\$41,500.00	0.0011%
R401 (PERSONAL CARE SERVICES)	\$21,730.78	0.0006%
R404 (PROF SVCS/LAND SURVEYS - CADASTRAL)	\$15,537.83	0.0004%
R609 (STENOGRAPHIC SERVICES)	\$11,027.12	0.0003%
R610 (PERSONAL PROPERTY MANAGEMENT SERVIC)	\$10,000.00	0.0003%
R712 (COIN MINTING)	\$8,280.00	0.0002%
R427 (PROF SVCS/WEATHER RPT-OBSERV)	\$3,300.00	0.0001%
<b>Total</b>	<b>\$3,686,873,417.49</b>	<b>100.00%</b>

<b>Question#:</b>	28
<b>Topic:</b>	contractors
<b>Hearing:</b>	Charting a Path Forward: The Homeland Security Department's Quadrennial Homeland Security Review and Bottom-Up Review
<b>Primary:</b>	The Honorable Claire McCaskill
<b>Committee:</b>	HOMELAND SECURITY (SENATE)

**Question:** I chaired a hearing for the Homeland Security and Governmental Affairs Subcommittee on Contracting Oversight on Counternarcotics Contracts in Latin America in May of this year. In preparation for this hearing I had requested documents from the Defense Department (DoD) and in order to respond, DoD hired a contractor to respond to our request. They paid the contractor almost \$50,000 to respond to a request from Congress; the contract ceiling was for \$150,000. Does DHS hire outside experts to respond to requests from Congress? Do you think that there are situations in which DHS should hire contractors to respond to requests from Congress? Please explain.

**Response:** Contractors are strictly prohibited from performing inherently governmental functions. Federal Acquisition Regulation § 7.503(c) provides a non-exhaustive list of examples of functions considered to be inherently governmental functions or which shall be treated as such. FAR § 7.503(c)(20) includes “[t]he drafting of Congressional testimony [and] responses to Congressional correspondence” as examples of inherently governmental functions. Supplementary Department-wide procedures in the Homeland Security Acquisition Manual (HSAM) sections 3007.502 and 3007.503 re-affirm FAR § 7.503(c)’s prohibitions.

There are, however, limited instances in which it may be appropriate for the Department to engage contractors for the purpose of *supporting* Federal employees drafting testimony and or responses to requests from Congress. The Department strives to provide Congress with complete, accurate, and timely responses to its requests. In order to achieve this important goal, it is occasionally necessary to enlist the labor of contractors in a support capacity, performing tasks such as research and data collection. In all cases, however, the drafting of testimony and responses to congressional questions and requests are conducted entirely by Federal employees.



# Quadrennial Homeland Security Review Report:

A Strategic Framework for a Secure Homeland

February 2010



Homeland  
Security

## TABLE OF CONTENTS

---

Letter From the Secretary .....	iii
Preface .....	v
Executive Summary .....	vii
I. Introduction .....	1
II. Today's Security Environment.....	5
III. Defining and Framing Homeland Security .....	11
IV. Overview of the Homeland Security Missions .....	19
Mission 1: Preventing Terrorism and Enhancing Security .....	21
Mission 2: Securing and Managing Our Borders.....	24
Mission 3: Enforcing and Administering Our Immigration Laws .....	27
Mission 4: Safeguarding and Securing Cyberspace.....	29
Mission 5: Ensuring Resilience to Disasters.....	31
Maturing and Strengthening the Homeland Security Enterprise .....	34
V. Missions, Goals, and Objectives of Homeland Security .....	37
Mission 1: Preventing Terrorism and Enhancing Security .....	38
Goal 1.1: Prevent Terrorist Attacks .....	38
Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities .....	40
Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events .....	41
Mission 2: Securing and Managing Our Borders .....	44
Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders.....	44
Goal 2.2: Safeguard Lawful Trade and Travel .....	46
Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations.....	48
Mission 3: Enforcing and Administering Our Immigration Laws.....	50
Goal 3.1: Strengthen and Effectively Administer the Immigration System .....	50
Goal 3.2: Prevent Unlawful Immigration .....	52
Mission 4: Safeguarding and Securing Cyberspace.....	54
Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment.....	54
Goal 4.2: Promote Cybersecurity Knowledge and Innovation .....	56
Mission 5: Ensuring Resilience to Disasters.....	59
Goal 5.1: Mitigate Hazards.....	59
Goal 5.2: Enhance Preparedness.....	60
Goal 5.3: Ensure Effective Emergency Response .....	62
Goal 5.4: Rapidly Recover .....	63



**TABLE OF CONTENTS**

---

VI. Maturing and Strengthening the Homeland Security Enterprise .....	65
VII. Conclusion: The Path Forward .....	77
Appendix A: Roles and Responsibilities Across the Homeland Security Enterprise .....	A-1
Appendix B: Quadrennial Homeland Security Review Process .....	B-1
Appendix C: Acronym List .....	C-1

Secretary

U.S. Department of Homeland Security  
Washington, DC 20528Homeland  
Security

Pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007*, I am pleased to submit the first Quadrennial Homeland Security Review (QHSR).

Since the terrorist attacks of September 11, 2001, this Nation has recognized how remote threats and distant trouble can pose near and present dangers to our shores. We have learned as a Nation that we must maintain a constant, capable, and vigilant posture to protect ourselves against new threats and evolving hazards. But we have also learned that vigilance and protection are not ends in and of themselves, but rather necessary tools in the service of our national purpose.

Just as today's threats to our national security and strategic interests are evolving and interdependent, so too must our efforts to ensure the security of our homeland reflect these same characteristics. As we develop new capabilities and technologies, our adversaries will seek to evade them, as was shown by the attempted terrorist attack on Flight 253 on December 25, 2009. We must constantly work to stay ahead of our adversaries.

This homeland security review addresses both the threats presented and the framework for our strategic response. The QHSR identifies the importance of what we refer to as the homeland security enterprise—that is, the Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population. The Department of Homeland Security (DHS) is one among many components of this national enterprise. In some areas, like securing our borders or managing our immigration system, the Department possesses unique capabilities and, hence, responsibilities. In other areas, such as critical infrastructure protection or emergency management, the Department's role is largely one of leadership and stewardship on behalf of those who have the capabilities to get the job done. In still other areas, such as counterterrorism, defense, and diplomacy, other Federal departments and agencies have critical roles and responsibilities, including the Departments of Justice, Defense, and State, the Federal Bureau of Investigation, and the National Counterterrorism Center. Homeland security will only be optimized when we fully leverage the distributed and decentralized nature of the entire enterprise in the pursuit of our common goals.

The purpose of this QHSR is to outline the strategic framework to guide the activities of participants in homeland security toward a common end. With respect to DHS specifically, the QHSR has led directly to

Quadrennial Homeland Security Review Report  
February 2010

Page iii

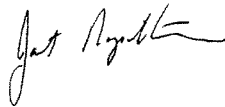
an examination of DHS's own activities from the bottom up in order to make recommendations regarding programs, assets, and capabilities, as well as policies, authorities, and organizational effectiveness, in its fiscal year 2012 budget submission. Thus, the QHSR will be followed by subsequent submissions to Congress that address programmatic, budgetary, and organizational alignment as called for by statute. The QHSR sets the stage by describing the breadth and depth of an enterprise-wide approach to homeland security.

In preparing the QHSR, the Department has benefited from the constructive engagement of thousands of dedicated individuals from across the country and, indeed, around the globe. Although numbers alone cannot capture the depth and vibrancy of the debates and discussions that occurred throughout the process of preparing the QHSR, more than 100 stakeholder associations and more than 500 experts from government at all levels, as well as academia and the private sector, have been engaged in this process. Our online National Dialogues had more than 20,000 visits, with over 3,000 comments submitted.

The QHSR reflects the most comprehensive assessment and analysis of homeland security to date. DHS worked closely with the White House, National Security Staff, and other Federal departments and agencies to refine the QHSR and ensure consistency with the President's 2010 National Security Strategy and other major security reviews, including the Quadrennial Defense Review and the Quadrennial Diplomacy and Development Review. This interagency engagement, at the leadership and staff levels, has helped to ensure that the QHSR represents the whole-of-government approach to national security envisioned by the Obama Administration.

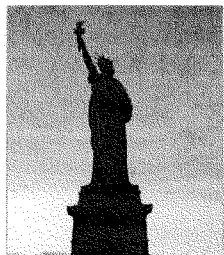
Indeed, every day, ensuring the security of the homeland requires the interaction of multiple Federal departments and agencies, as well as operational collaboration across Federal, State, local, tribal, and territorial governments, nongovernmental organizations, and the private sector. This collaboration and cooperation undergirds our security posture at our borders and ports, our preparedness in our communities, and our ability to effectively react to crises. The QHSR makes specific recommendations on how to strengthen and mature the homeland security enterprise, including mechanisms to enhance unity of effort across multiple homeland security partners and stakeholders.

Finally, in presenting this first-ever QHSR, I believe it is important to acknowledge the efforts and commitment of my predecessors in this office, the men and women of the Department of Homeland Security, and the many thousands of law enforcement personnel, first responders, emergency managers, and other homeland security professionals across the country who have worked tirelessly to make this Nation secure. On their behalf, and on behalf of those who continue to serve, I am pleased to deliver this first Quadrennial Homeland Security Review.



Secretary Janet Napolitano

## PREFACE



The first-ever Quadrennial Homeland Security Review (QHSR) comes amid much expectation and interest. Homeland security encompasses the most sweeping reform in government in nearly half a century, and makes explicit the realization that the evolving international security landscape bears directly on our domestic security. But we have also learned that security is not an end in itself; rather, it is an important means to a vital end: preserving the values, principles, and way of life we pursue as Americans.

A review of homeland security could take many forms—from a retrospective and assessment of the past, to an analysis of current programs and activities, to a view of what the future might bring. Nonetheless, Congress made clear in its direction to the Department of Homeland Security (DHS), the principal author of this report, that the QHSR should delineate a homeland security strategy, including an outline of priority mission areas, not simply for DHS, but for the homeland security enterprise as a whole—embracing Federal, State, local, tribal, and territorial governments, nongovernmental organizations, the private sector, as well as individuals, families and communities. Such a strategic analysis would then serve as a basis for a deeper review of the many programs and budgets required to execute the full range of homeland security missions.

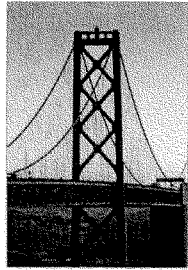
Congress also sought to better understand the resource and organizational implications of an evolving strategic view of homeland security. What was clear from the start, however, is that any articulation of strategy or analysis of specific programmatic or resource tradeoffs—either within DHS or across the broader homeland security enterprise—had to be firmly rooted within a comprehensive strategic understanding of homeland security. For example, “What is homeland security?” “How is the homeland best made secure?” “What does it mean to be prepared?” Eight years after 9/11, these questions still echo widely among the many homeland security stakeholders.

The QHSR marks the beginning of a multi-step process to answer these questions. It offers a vision for a secure homeland, specifies key mission priorities, outlines goals for each of those mission areas, and lays the necessary groundwork for subsequent analysis and recommendations. As an immediate follow-on and complement to the QHSR, an important “bottom-up” review of DHS was begun in November 2009 that will look to align the Department’s programmatic activities and organizational structure with the mission sets and goals identified in the QHSR. That review is scheduled to be completed in the first calendar quarter of 2010.

## PREFACE

While the primary purpose for the QHSR is to outline the strategic framework to guide the activities of participants in homeland security toward a common end, it is equally important to note what the QHSR is *not*. The report is not a resource prioritization document, although in identifying key mission areas for priority focus, it is highly indicative of where those priorities should lie. Nor does the QHSR detail the roles and responsibilities of Federal or other institutions for each mission area. Instead, the QHSR functions as a strategic document that seeks to answer the most fundamental questions that many Americans still ask about homeland security. By describing a forward-looking homeland security vision for the Nation and the requisite set of key mission areas, goals, objectives, and outcomes, integrated across the breadth of the homeland security landscape, it also will serve as a roadmap to keep America safe, secure, and resilient in the years ahead.

## EXECUTIVE SUMMARY



The purpose of the first-ever Quadrennial Homeland Security Review (QHSR) is to outline the strategic framework to guide the activities of participants in homeland security toward a common end. A safe and secure homeland must mean more than preventing terrorist attacks from being carried out. It must also ensure that the liberties of all Americans are assured, privacy is protected, and the means by which we interchange with the world—through travel, lawful immigration, trade, commerce, and exchange—are secured.

In addition, while the importance of preventing another terrorist attack in the United States remains undiminished, much has been learned since September 11, 2001, about the range of challenges we face. Hurricane Katrina, widespread international cyber attacks, the expansion of transnational criminal activities, and H1N1 influenza are examples of threats and hazards that are central to homeland security, requiring an equally wide variety of capabilities to address them.

The QHSR is not simply a discussion of the roles and responsibilities of the Department of Homeland Security (DHS).<sup>1</sup> The QHSR acknowledges existing relationships, roles, and responsibilities, and seeks to set forth a shared vision of homeland security in order to achieve unity of purpose. The Nation's first QHSR takes as its aim a vision for our homeland as safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

### *Today's Security Environment*

The accelerated flow of ideas, goods, and people around the world, while vital to supporting and advancing America's interests, also creates security challenges that are increasingly borderless and unconventional. To a greater degree than at any point in history, individuals and small groups—from nongovernmental organizations (NGOs) on the one hand to criminal networks and terrorist organizations on the other—have the ability to engage the world with far-reaching effects, including those that are disruptive and destructive.

Among the forces that threaten the United States and its interests are those that blend the lethality and high-tech capabilities of modern weaponry with the power and opportunity of asymmetric tactics such as terrorism and cyber warfare. We are

<sup>1</sup> Section 707 of the Homeland Security Act of 2002, as amended, requires the Secretary of Homeland Security, in each quadrennial review, to "delineate and update, as appropriate, the national homeland security strategy," and to "outline and prioritize the full range of the critical homeland security mission areas of the Nation."

## EXECUTIVE SUMMARY

challenged not only by novel employment of conventional weaponry, but also by the hybrid nature of these threats. We have seen their effects on the American homeland. Moreover, we must remember that we face a determined and constantly adapting adversary. The attempted terrorist attack on Flight 253 on December 25, 2009, is a powerful illustration that terrorists will go to great lengths to try to defeat the security measures that have been put in place since 9-11.

Figure ES-1. Threats, Hazards, and Long-Term Global Challenges and Trends

Threats and Hazards	Global Challenges and Trends
<ul style="list-style-type: none"> <li>• High-consequence weapons of mass destruction</li> <li>• Al-Qaeda and global violent extremism</li> <li>• High-consequence and/or wide-scale cyber attacks, intrusions, disruptions, and exploitations</li> <li>• Pandemics, major accidents, and natural hazards</li> <li>• Illicit trafficking and related transnational crime</li> <li>• Smaller scale terrorism</li> </ul>	<ul style="list-style-type: none"> <li>• Economic and financial instability</li> <li>• Dependence on fossil fuels and the threats of global climate change</li> <li>• Nations unwilling to abide by international norms</li> <li>• Sophisticated and broadly available technology</li> <li>• Other drivers of illicit, dangerous, or uncontrolled movement of people and goods</li> </ul>

### *Defining and Framing Homeland Security*

Homeland security describes the intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defense, emergency response, law enforcement, customs, border control, and immigration. In combining these responsibilities under one overarching concept, homeland security breaks down longstanding stovepipes of activity that have been and could still be exploited by those seeking to harm America. Homeland security also creates a greater emphasis on the need for joint actions and efforts across previously discrete elements of government and society.

Homeland security is a widely distributed and diverse—but unmistakable—national enterprise. The term “enterprise” refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. The use of the term connotes a broad-based community with a common interest in the public safety and well-being of America and American society that is composed of multiple actors and stakeholders

## EXECUTIVE SUMMARY

whose roles and responsibilities are distributed and shared. As the Commander-in-Chief and the leader of the Executive Branch, the President of the United States is uniquely responsible for the safety, security, and resilience of the Nation. The White House leads overall homeland security policy direction and coordination. Individual Federal agencies, in turn, are empowered by law and policy to fulfill various aspects of the homeland security mission. The Secretary of Homeland Security leads the Federal agency as defined by statute charged with homeland security: preventing terrorism and managing risks to critical infrastructure; securing and managing the border; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. However, as a distributed system, no single entity is responsible for or directly manages all aspects of the enterprise.

There are three key concepts that are essential to, and form the foundation for, a comprehensive approach to homeland security:

- **Security:** Protect the United States and its people, vital interests, and way of life;
- **Resilience:** Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery; and
- **Customs and Exchange:** Expedite and enforce lawful trade, travel, and immigration.

All homeland security activities must be built upon a foundation of ensuring security and resilience, as well as facilitating the normal, daily activities of society and interchange with the world.

### *The Homeland Security Missions*

The QHSR outlines the Nation's homeland security missions, or broad areas of activity around which the homeland security enterprise is oriented. *These missions are enterprise-wide, and not limited to the Department of Homeland Security.* Hundreds of thousands of people from across the Federal Government, State, local, tribal, and territorial governments, the private sector, and other nongovernmental organizations are responsible for executing these missions. These homeland security professionals must have a clear sense of what it takes to achieve the overarching vision.



## EXECUTIVE SUMMARY

There are five homeland security missions. The missions and associated goals are as follows:

### **Mission 1: Preventing Terrorism and Enhancing Security**

- Goal 1.1: Prevent Terrorist Attacks
- Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
- Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events

### **Mission 2: Securing and Managing Our Borders**

- Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders
- Goal 2.2: Safeguard Lawful Trade and Travel
- Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

### **Mission 3: Enforcing and Administering Our Immigration Laws**

- Goal 3.1: Strengthen and Effectively Administer the Immigration System
- Goal 3.2: Prevent Unlawful Immigration

### **Mission 4: Safeguarding and Securing Cyberspace**

- Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
- Goal 4.2: Promote Cybersecurity Knowledge and Innovation

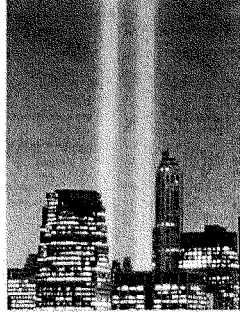
### **Mission 5: Ensuring Resilience to Disasters**

- Goal 5.1: Mitigate Hazards
- Goal 5.2: Enhance Preparedness
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Rapidly Recover

In addition, we must specifically focus on maturing the homeland security enterprise itself. Maturing and strengthening the homeland security enterprise includes enhancing shared awareness of risks and threats, building capable communities, fostering unity of effort, and fostering innovative approaches and solutions through leading-edge science and technology.

By defining the homeland security missions and setting prioritized goals, objectives, and strategic outcome statements for each mission, we chart a course for action over the next 4 years.

## I. INTRODUCTION



The story of homeland security is inextricably linked to the story of 9/11. The vivid images of the World Trade Center, the Pentagon, and smoldering fields in Shanksville, Pennsylvania, portrayed a Nation obviously shaken by the catastrophic surprise attacks that had occurred on its soil. Yet on that same day there were other images—of firefighters racing up the stairs of the Twin Towers, of police and first responders rushing aid to those in need at the Pentagon, and of ordinary Americans, indeed total strangers, coming together to help each other cope with challenges large and small. These images of American resilience portrayed a Nation determined to do whatever it might take to recover from this disaster and to prevent such attacks from occurring again.

In the closing days of 2001, the first narrative describing homeland security began to take shape: that despite the dramatic changes since the end of the Cold War, the world was still very much a dangerous place. The terrorists that had targeted this country clearly were determined to attack Americans at home, American interests anywhere, and our friends and allies everywhere. As the central part of this first narrative, our Nation believed that it needed to improve its vigilance, increase its preparedness, reduce its vulnerabilities, and strengthen its guard against any future attack in order to confront this threat.

The Federal Government began to institutionalize these priorities with a series of initiatives under the banner of *homeland security*: a Presidential advisor and advisory council were appointed, a series of national-level policies were issued, new statutory authorities were enacted by Congress, and in 2003, a new Federal agency was established—the Department of Homeland Security (DHS). These initiatives—in particular, the newly established DHS—linked the imperative of safeguarding the Nation to key operational responsibilities that were principally focused on securing the Nation's borders and air transportation system, while enhancing the Nation's preparedness to confront terrorism.

In the years since 9/11, homeland security has become commonly and broadly known as both a term and as a Federal department. Less well understood, however, has been its ongoing purpose and function. What is homeland security? Is it more than preventing terrorism? If so, what else does it take to achieve a safe and secure homeland? What risks are we willing to accept? Who has the responsibility, authority, capabilities, and resources to do all that needs doing?

The attempted terrorist attack on Flight 253 on December 25, 2009, demonstrates that al-Qaeda continues to plot against us, and thus, the importance of preventing another

## I. INTRODUCTION

terrorist attack in the United States remains undiminished. However, much has been learned since 9/11 about the range of additional challenges we face. Hurricane Katrina powerfully illustrated the overall impact of weak preparedness and response in the face of extreme natural disasters. Widespread international cyber attacks—from some of the most sophisticated denial-of-service efforts to persistent and rising attacks on U.S. Government cyber systems—reflect the increasing importance of securing the information systems that are the very lifeblood of so much of our critical energy, financial, health, commerce, and transportation infrastructure. Transnational criminal organizations that have expanded efforts to cross our borders with illicit goods, currency, and trafficked persons represent a growing threat to the prosperity, security, and quality of life of U.S. citizens at home and abroad. As we have seen with H1N1 influenza, the rapid global spread of infectious diseases can cause great disruptions at home. Preventing these and other dangers from threatening our Nation has also become central to homeland security.

At the same time, we have learned that it is not possible to secure the American homeland simply with physical protections or through strategies that reinforce fear or isolation. Nor is this country made safe by substantially curtailing the very rights and liberties that define the free and diverse society we seek to protect, or by excluding visitors and lawful immigrants. Indeed, homeland security is as much about protecting the American way of life as it is about protecting this country from future attacks.

Thus, a safe and secure homeland must mean more than preventing terrorist attacks from being carried out. It must also ensure that the liberties of all Americans are assured, privacy is protected, and the means by which we interchange with the world—through travel, lawful immigration, trade, commerce, and exchange—are secured. Ultimately, homeland security is about effectively managing risks to the Nation's security. As such, an effective strategy for homeland security forms an important component of our overarching national security strategy.

**“We reject as false the choice between our safety and our ideals. Our Founding Fathers, faced with perils we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man, a charter expanded by the blood of generations. Those ideals still light the world, and we will not give them up for expedience’s sake.”**

**– President Barack Obama**

## I. INTRODUCTION

The purpose of this first-ever Quadrennial Homeland Security Review (QHSR) is to elaborate upon this broader vision by outlining the strategic framework to guide the activities of participants in homeland security toward a common end. And in this regard, it is important to note that this is not a review confined to the roles and responsibilities of DHS.<sup>3</sup> Homeland security encompasses a much broader scope, with vital contributions from all Federal agencies, State, local, tribal, and territorial governments, businesses, and nongovernmental organizations, as well as individuals, families, and communities. International partnerships are also essential to success.

Thus, this QHSR will describe more comprehensively the Nation's homeland security interests, identify more clearly the critical homeland security missions, and define more completely a strategic approach to those missions by laying out the principal goals, essential objectives, and key strategic outcomes necessary for that strategic approach to succeed. The QHSR acknowledges existing relationships and roles and responsibilities, and seeks to set forth a shared vision of homeland security in order to achieve unity of purpose going forward.

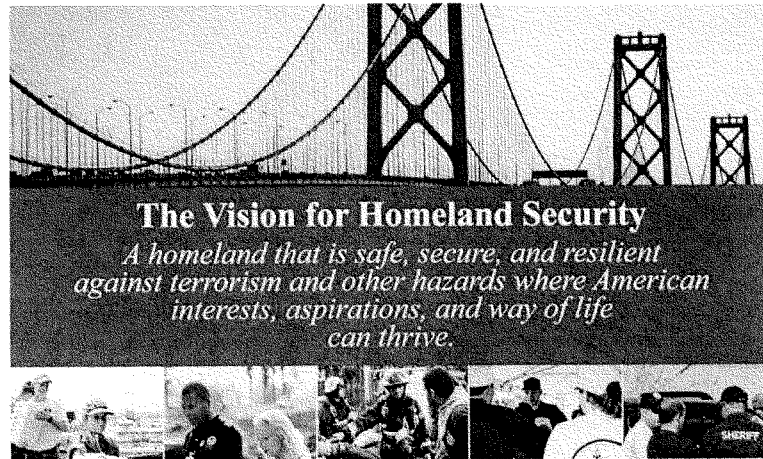
When we recall the events of 9/11, we are reminded of the destruction of those attacks to be sure. However, as we look forward from this vantage point, it is essential that we elevate the importance of the extraordinary acts that also took place when New York firefighters marched up tower stairs, when passengers of United Flight 93 stormed the cockpit and sacrificed their lives, and when countless fellow citizens across the country volunteered their time for days and months on end to help others heal. These stories of the bravery, courage, and resolve of the American people tell the story of homeland security.

These acts of courage also demonstrate the simple yet profound truth: that homeland security is not simply about government action alone, but rather about the collective strength of this entire country. The Nation's first QHSR builds on the conviction that this country can protect itself and takes as its aim a vision for our homeland as safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

---

<sup>3</sup> Section 707 of the Homeland Security Act of 2002, as amended, requires the Secretary of Homeland Security, in each quadrennial review, to "delineate and update, as appropriate, the national homeland security strategy," and to "outline and prioritize the full range of the critical homeland security mission areas of the Nation."

## I. INTRODUCTION



## II. TODAY'S SECURITY ENVIRONMENT



The interconnected nature of people, economies, and international infrastructure around the world can infuse seemingly isolated or remote events with global consequences. Events at home and abroad generate rapid effects, often in an interconnected fashion, driven by breathtaking technological change and speed-of-light international communications. This accelerated flow of ideas, goods, and people around the world, while vital to supporting and advancing America's interests, also creates security challenges that are increasingly borderless and unconventional.

In many parts of the world, states no longer have a monopoly on the use of force, although they continue to hold a large majority of power. Globally, natural hazards have increased in scale and impact, and emerging diseases move effortlessly across borders and expansively through global movement systems. To a greater degree than at any point in history, individuals and small groups—from nongovernmental organizations (NGOs) on the one hand, to criminal networks and terrorist organizations on the other—have the ability to engage the world with far-reaching effects, including those that are disruptive and destructive.

Homeland security, as an essential element of our Nation's security, must be firmly embedded in and linked to broader national security concerns. Against this backdrop, we must pursue a homeland security agenda linked to America's national security interests. Such interests reflect the Nation's highest order priorities.

America's interests are inextricably linked to the integrity and resilience of the international system. Chief among these interests are security, prosperity, broad respect for universal values, and an international order that promotes cooperative action. Consistent with the President's vision, the United States will advance these interests by strengthening our domestic foundation and integrating all elements of national power, engaging abroad on the basis of mutual interest and mutual respect, and promoting an international order that reinforces the rights and responsibilities of all nations.

## II. TODAY'S SECURITY ENVIRONMENT

Among the forces that threaten the United States and its interests are those that blend the lethality and high-tech capabilities of modern weaponry with the power and opportunity of asymmetric tactics such as terrorism and cyber warfare. We are challenged not only by novel employment of conventional weaponry, but also by the

hybrid nature of these threats. Countering such threats requires us to adapt traditional roles and responsibilities across the national security spectrum and craft solutions that leverage the capabilities that exist both inside and outside of government. The attempted terrorist attack on Flight 253 on December 25, 2009, powerfully illustrates that terrorists will go to great lengths to try to defeat the security measures that have been put in place since 9/11.

More specifically, the threats and hazards that challenge U.S. interests from a homeland security perspective include:

- High-consequence weapons of mass destruction (WMD), in particular, improvised nuclear devices and high-consequence biological weapons, which would have the greatest potential effects if used against the United States. We know that non-state actors actively seek to acquire, build, and use such weapons and technologies, and that foreign states continue to develop high-consequence weaponry with the intent to intimidate or blackmail the international community and proliferate to other potentially hostile state or non-state actors. Dangerous materials, technology, and know-how circulate with ease in our globalized economy and are controlled unevenly around the world, raising the possibility of theft or accidental use and making it difficult to track and prevent proliferation.
- Al-Qaeda and global violent extremism, which directly threaten the United States and its allies. Terrorist networks exploit gaps in governance and security within both weak and advanced states. Some terrorist organizations benefit from active state-sponsorship and from the failure of other states to counter known terrorist organizations or sources of support within their borders. Terrorist organizations have expressed the intent to employ mass-casualty WMD as well as smaller scale attacks against prominent political, economic, and infrastructure targets in the United States and around the world.

**Hybrid threats** refer to the ability of adversaries—lone attackers, criminals, transnational terrorist organizations, even nation-states—to employ combinations of tactics, technologies, and capabilities to gain an asymmetric advantage.

**“We will . . . relentlessly confront violent extremists** who pose a grave threat to our security—because we reject the same thing that people of all faiths reject: the killing of innocent men, women, and children.”

– President Barack Obama

## II. TODAY'S SECURITY ENVIRONMENT

- High-consequence and/or wide-scale cyber attacks, intrusions, disruptions, and exploitations, which, when used by hostile state or non-state actors, could massively disable or impair critical international financial, commercial, physical, and other infrastructure. This in turn could cripple the global movement of people and goods worldwide and bringing legitimate and vital social and economic processes to a stand-still. These cyber attacks involve individuals and groups who conduct intrusions in search of information to use against the United States, and those who spread malicious code in an attempt to disrupt the national information infrastructure.
- Pandemics, major accidents, and natural hazards, which can result in massive loss of life and livelihood equal to or greater than many deliberate malicious attacks. Certain public health threats, such as disease outbreaks and natural hazards (e.g., hurricanes and floods), occur organically. Others can be introduced into the United States through the movement of people and goods across our borders.
- Illicit trafficking and related transnational crime, which can undermine effective governance and security, corrupt strategically vital markets, slow economic growth, and destabilize weaker states. Transnational crime and trafficking facilitate the movement of narcotics, people, funds, arms, and other support to hostile actors, including terrorist networks. Importantly for the American homeland, the dramatic detrimental effect of illegal trafficking and transnational criminal organizations is apparent in societies within the Western Hemisphere.
- Smaller scale terrorism, which may include violent extremists and other state or non-state actors conducting small-scale explosive and cyber attacks and intrusions against population centers, important symbolic targets, or critical infrastructure.

In addition to these specific threats and hazards, America's national interests are also threatened by global challenges and long-term trends. These include:

- Economic and financial instability, that can undermine confidence in the international order, fuel global political turbulence, and induce social and political instability in weak states abroad.
- Dependence on fossil fuels and the threat of global climate change that can open the United States to disruptions and manipulations in energy supplies and to changes in our natural environment on an unprecedented scale. Climate change is expected to increase the severity and frequency of weather-related hazards, which could, in turn, result in social and political destabilization, international conflict, or mass migrations.



## II. TODAY'S SECURITY ENVIRONMENT

- Nations unwilling to abide by international norms that can threaten U.S. security interests directly or indirectly by sponsoring terrorism, encouraging WMD proliferation, serving as a source of cyber disruptions, committing human rights atrocities, or providing safe haven to transnational criminal networks.
- Sophisticated and broadly available technology, which empowers our adversaries. We must adapt our intelligence and counterintelligence practices to defeat hostile operations and the use of intelligence tradecraft by small groups and individuals planning destructive attacks against the homeland.
- Other drivers of illicit, dangerous, or uncontrolled movement of people and goods, including fragile and failing states, regional instability, competition for resources, demographic shifts, environmental degradation, genocide, and other gross violations of human rights. These same drivers can also foster terrorism and violent extremist ideology, breed transnational crime, and facilitate the proliferation of high-consequence weaponry.

The national security of the United States depends on a comprehensive approach to preserve and advance our interests while managing the risks posed by the threats outlined above. An effective strategy for homeland security forms an important component of our overarching national security strategy, and three assumptions in particular shape its development.

First, rapid technological change will continue to alter social, economic, and political forces, rapidly disperse information, and provide new means for our adversaries and competitors to challenge us. The increasing interconnectivity of infrastructure and its dependence on cyber systems creates opportunities for adversaries to use cyber tools to attack critical infrastructure and gain access to government, business, and personal information systems. Second, multiple simultaneous crises will likely challenge the Nation and its resources, requiring all stakeholders to be capable of managing crises including some for extended periods. Multiple simultaneous crises will also place a premium on all stakeholders' knowledge of and ability to use incident management protocols and procedures, and will challenge national priority setting and resource allocation demands. Finally, we must guard against the danger of complacency as memories of the 9/11 attacks and other major crises recede. The failed airline plot of December 25, 2009, serves to heighten our vigilance, but we know that readiness is costly and requires sustained commitment.

## II. TODAY'S SECURITY ENVIRONMENT

### Assumptions Concerning the Security Environment

- **Violent extremist groups**, including potential homegrown extremists, will continue to use terrorism to attack U.S. targets;
- Technologies associated with WMD, often dual-use, will circulate easily in a globalized economy, challenging traditional **WMD nonproliferation and counterproliferation efforts**, especially in the nuclear and biological areas;
- Terrorists, proliferators, and other criminal elements will seek to take advantage of the **increasingly globalized financial system** and its legitimate and beneficial functions to move money in support of their dangerous conduct;
- Economic crises and disparities will continue to induce social and/or political instability, in some cases increasing **migrant and refugee flows—legal and illegal—into the United States**;
- Globalization will continue to make it increasingly difficult to prevent **health threats to the United States**, whether from emerging disease or deliberate attacks, or via imports;
- **Technological change and cyber threats** from state and non-state actors will continue to alter social, economic, and political forces, allow for the rapid dissemination of information, and provide new means for adversaries to challenge the United States;
- **Climate change** will increase the severity and frequency of weather-related hazards such as extreme storms, high rainfalls, floods, droughts, and heat waves;
- The security environment will continue to pose the potential for **multiple simultaneous crises**; and
- There is a danger of **complacency** as major crises recede.

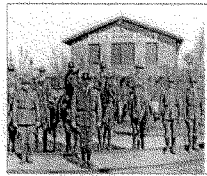
This page intentionally left blank.

### III. DEFINING AND FRAMING HOMELAND SECURITY



Because the term is in such widespread use, it may be easy today to overlook the fact that *homeland security* is a relatively new concept. Yet it is one that can trace its roots to traditional functions such as civil defense, emergency response, law enforcement, customs, border control, and immigration.

Homeland security captures the effort to adapt these traditional functions to confront new threats and evolving hazards.



While homeland security is still relatively new, it may be useful to recall that the concept of *national security* was also little known until the 1930s, and was only formally established as an organizing principle after World War II. The *National Security Act of 1947* brought together the Department of War and the Department of the Navy into a single integrated entity that became the Department of Defense. The act also created the National Security Council and a position on the President's staff that would later become the National Security Advisor. The innovation was to bring together under one overall concept the consideration of foreign affairs and military policy, which had been, up until that time, two largely separate governmental domains. Over the decades, aspects of economic policy, trade policy, energy policy, and countering transnational threats were also drawn into the ambit of national security.



In 2002, the *Homeland Security Act* sought to integrate the various elements of homeland security in a similar manner, creating both the Department of Homeland Security and the Homeland Security Council. In effect, the 2002 *Homeland Security Act* added a third concept to the military and foreign affairs pillars of national security by associating domestic security concerns with national security.



Homeland security describes the intersection of evolving threats and hazards with the traditional governmental and civic responsibilities of civil defense, emergency response, law enforcement, customs, border control, and immigration. In combining these responsibilities under one overarching concept, homeland security breaks down longstanding stovepipes of activity that could be exploited by those seeking to harm America. Homeland security also creates a greater emphasis on and need for joint actions and efforts across previously discrete elements of government and society.

### III. DEFINING AND FRAMING HOMELAND SECURITY

#### *The Homeland Security Enterprise*

Given this historical context, the question “What is homeland security?” recognizes that, in fact, securing the United States and its people represents an overarching national objective. Equally important, and aside from obviously identifying a Cabinet-level department of the Federal Government, homeland security is a widely distributed and diverse—but unmistakable—national enterprise.

The term “enterprise” refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It

connotes a broad-based community with a common interest in the public safety and well-being of America and American society and is composed of multiple partners and stakeholders whose roles and responsibilities are distributed and shared. Yet it is important to remember that these partners and stakeholders face diverse risks, needs, and priorities. The challenge for the enterprise, then, is to balance these diverse needs and priorities, while focusing on our shared interests and responsibilities to collectively secure our homeland.

As the Commander-in-Chief and the leader of the Executive Branch, the President of the United States is uniquely responsible for the safety, security, and resilience of the Nation. The White House leads overall homeland security policy direction and coordination. Individual Federal agencies, in turn, are empowered by law and policy to fulfill various aspects of the homeland security mission. The Secretary of Homeland Security leads the Federal agency as defined by statute charged with homeland security: preventing terrorism and managing risks to critical infrastructure; securing and managing the border; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters. In some areas, like securing our borders or managing our immigration system, the Department of Homeland Security possesses unique capabilities and, hence, responsibilities. In other areas, such as critical infrastructure protection or emergency management, the Department’s role is largely one of leadership and stewardship on behalf of those who have the capabilities to get the job done. In still other areas, such as counterterrorism, defense, and diplomacy, other Federal

#### **The homeland security “enterprise”**

refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. It connotes a broad-based community with a common interest in the safety and well-being of America and American society.

### III. DEFINING AND FRAMING HOMELAND SECURITY

departments and agencies have critical leadership roles and responsibilities, including the Departments of Justice, Defense, and State, the Federal Bureau of Investigation, and the National Counterterrorism Center. State, local, tribal, and territorial governments all play vital roles in protecting the homeland. Homeland security will only be successful when we fully leverage the distributed and decentralized nature of the entire enterprise in the pursuit of our common goals.

Therefore, key leadership responsibilities to achieve our homeland security missions are discharged through engagement and collaboration with the vast array of homeland security enterprise partners and stakeholders. As a distributed system, no single entity is responsible for or directly manages all aspects of the enterprise. Different agencies and offices direct and lead specific homeland security activities at the Federal, State, local, tribal, and territorial levels, as well as within the private sector—and between and among all of these entities—for the full range of homeland security purposes. And because responsibilities are distributed, entities that provide direction and leadership in one instance may play supporting roles in another.

**Appendix A** reflects the current alignment of roles and responsibilities across the enterprise.

With the establishment of homeland security, and the linking of domestic security concerns to broader national security interests and institutions, there is a temptation to view homeland security so broadly as to encompass all national security and domestic policy activities. This is not the case. Homeland security is deeply rooted in the security and resilience of the Nation, and facilitating lawful interchange with the world. As such, it intersects with many other functions of government. Homeland security is built upon critical law enforcement functions, but is not about preventing all crimes or administering our Nation's judicial system. It is deeply embedded in trade activities, but is neither trade nor economic policy. It requires international engagement, but is not responsible for foreign affairs. Rather, homeland security is meant to connote a concerted, shared effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.

*Homeland security is a concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.*

### III. DEFINING AND FRAMING HOMELAND SECURITY

#### *The Evolution of Homeland Security*

As noted earlier, although the integrated concept of homeland security arose at the turn of the 21<sup>st</sup> century, homeland security traces its roots to concepts that originated with the founding of the Republic. Homeland security describes the intersection of new threats and evolving hazards with traditional governmental and civic responsibilities for civil defense, emergency response, customs, border control, law enforcement, and immigration. Homeland security draws on the rich history, proud traditions, and lessons learned from these historical functions to fulfill new responsibilities that require the engagement of the entire homeland security enterprise and multiple Federal departments and agencies.

Figure 1. The Evolution of Homeland Security



#### *The Key Concepts of Homeland Security*

For the past 7 years, homeland security has rested on four key activities—prevention, protection, response, and recovery—oriented principally against the threat of terrorism. Preventing a terrorist attack in the United States remains the cornerstone of homeland security. It is clear, however, that this emphasis on terrorism does not capture the full range of interconnected threats and challenges that characterize today's world. A robust notion of homeland security must take account of our essential need to safely, securely, and intensively engage the rest of the world—through trade, travel, and other exchanges. In other words, a place where the American way of life can thrive.

Three key concepts form the general foundation for a comprehensive approach to homeland security going forward: Security, Resilience, and Customs and Exchange.

### III. DEFINING AND FRAMING HOMELAND SECURITY

**Security:** Protect the United States and its people, vital interests, and way of life. Homeland security relies on our shared efforts to prevent and deter attacks by identifying and interdicting threats, denying hostile actors the ability to operate within our borders, and protecting the Nation's critical infrastructure and key resources. Initiatives that strengthen our protections, increase our vigilance, and reduce our vulnerabilities remain important components of our security. This is not to say, however, that security is a static undertaking. We know that the global systems that carry people, goods, and data around the globe also facilitate the movement of *dangerous* people, goods, and data, and that within these systems of transportation and transaction, there are key nodes—for example, points of origin and transfer, or border crossings—that represent opportunities for interdiction. Thus, we must work to confront threats at every point along their supply chain—supply chains that often begin abroad. To ensure our homeland security then, we must engage our international allies, and employ the full breadth of our national capacity—from the Federal Government, to State, local, tribal, and territorial police, other law enforcement entities, the Intelligence Community, and the private sector—and appropriately enlist the abilities of millions of American citizens.

**“The terrorists have used our open society against us. In**

wartime, government calls for greater powers, and then the need for those powers recedes after the war ends. This struggle will go on. Therefore, while protecting our homeland, Americans should be mindful of the threats to vital personal and civil liberties. This balancing is no easy task, but we must constantly strive to keep it right. This shift of power and authority to the government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life.”

– The 9/11 Commission Report

**Resilience:** Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery. Our country and the world are underpinned by interdependent networks along which the essential elements of economic prosperity—people, goods and resources, money, and information—all flow. While these networks reflect progress and increased efficiency, they are also sources of vulnerability. The consequences of events are no longer confined to a single point: a disruption in one place can ripple through the system and have immediate, catastrophic, and multiplying consequences across the country and around the world.

Despite our best efforts, some attacks, accidents, and disasters will occur. Therefore, the challenge is to foster a society that is robust, adaptable, and has the capacity for rapid recovery. In this context, individuals, families, and communities—and the systems that sustain them—must be informed, trained, and



### III. DEFINING AND FRAMING HOMELAND SECURITY

materially and psychologically prepared to withstand disruption, absorb or tolerate disturbance, know their role in a crisis, adapt to changing conditions, and grow stronger over time.

**“Our goal** is to ensure a more resilient Nation—one in which individuals, communities, and our economy can adapt to changing conditions as well as withstand and rapidly recover from disruption due to emergencies.”

— President Barack Obama

This concept is not new, and different eras in our history reflect an unwavering focus on building national resilience. The history of civil defense in the United States, for example, is marked by sweeping national debates about concepts that, if not by name, were nevertheless entirely about resilience. Notable among these was the debate spanning the Truman and Eisenhower administrations about whether to expend resources on sheltering individuals in the face of nuclear attack or to focus investments in a national highway system to

facilitate mass evacuation of urban populations. These issues were beset with the same challenges that confront us today, including how to foster a decentralized approach to security, and how to best meet the challenge of helping our citizens prepare psychologically and materially for attacks and disasters that do occur. The rapid evolution of national security threats and the arrival of the information age have increased the urgency of building up—and reemphasizing—our historically resilient posture.

**Customs and Exchange: Expedite and enforce lawful trade, travel, and immigration.** The partners and stakeholders of the homeland security enterprise are responsible for facilitating and expediting the lawful movement of people and goods into and out of the United States. This responsibility intersects with and is deeply linked to the enterprise’s security function. We need a smarter, more holistic approach that embeds security and resilience directly into global movement systems. Strengthening our economy and promoting lawful trade, travel, and immigration must include security and resilience, just as security and resilience must include promoting a strong and competitive U.S. economy, welcoming lawful immigrants, and protecting civil liberties and the rule of law. We view security along with customs and exchange as mutually reinforcing and inextricably intertwined through actions such as screening, authenticating, and maintaining awareness of the flow of people, goods, and information around the world and across our borders.

### III. DEFINING AND FRAMING HOMELAND SECURITY

#### Customs in Historical Context

After declaring independence, the United States found itself on the brink of bankruptcy. To raise revenue, the second act of Congress—the *Tariff Act of 1789*—authorized the first Secretary of the Treasury, Alexander Hamilton, to collect duties on imported goods. A month later, in its fifth act, Congress established 59 customs collection districts around the country and designated ports of entry under the jurisdiction of the Department of the Treasury's Collectors of Customs.

From inception, the Collectors of Customs were given numerous responsibilities designed to support the collection of customs revenue. Recognizing that revenue would increase if more ships could make it to port safely and quickly, Congress immediately created the Lighthouse Service, which eventually came under Collectors of Customs authority, to construct and maintain all navigational aids. To assist in the collection of duties and tonnage taxes, and to combat smuggling by privateers, which negatively impacted revenue collection, a maritime law enforcement arm was added a year later—the U.S. Revenue Marine. As the Nation's land borders expanded, the U.S. Customs Border Patrol was created to address smuggling between ports of entry.

The Collectors of Customs were assigned other tasks that were inherently intertwined with their customs responsibilities. Because their ships already patrolled the coastline, the Revenue Marine assumed responsibility for maritime security and, in the 1840s with its acquisition of the Life Saving Service, maritime safety. The Collectors of Customs were also charged with implementing immigration policy and enforcing immigration law, because they were representatives of the Federal Government at ports of entry. By 1853, the Collectors of Customs had authority over customs and immigration law enforcement, maritime safety and security, and border security.

Beginning in the late 1800s, however, the Collectors of Customs structure was reorganized. In 1871, the Revenue Marine (which had been renamed the Revenue Cutter Service) and Life Saving Service were removed from Collectors of Customs authority. The two organizations combined in 1915 to form the U.S. Coast Guard. In 1891, Congress moved the Collectors' immigration functions to the Office of the Superintendent of Immigration, which later evolved into the Immigration and Naturalization Service. By the turn of the century, the Collectors of Customs (eventually renamed the U.S. Customs Service) had become an organization focused solely on customs enforcement and antismuggling. Around the same time, growing income from excise taxes and, in 1913, an income tax meant that customs duties were no longer the primary source of Federal Government revenue.\* The facilitation of commerce and immigration in support of overall economic growth became a substantial priority alongside the collection of customs revenue.

For the next 100 years, customs and immigration enforcement, border security, and maritime safety and security functions remained distributed across multiple agencies within three cabinet departments—the Department of the Treasury (customs), the Department of Justice (immigration enforcement and border security), and the Department of Transportation (maritime safety and security). The creation of the Department of Homeland Security (DHS) in 2003 reunited these long interrelated and mutually supportive functions. Every day as part of DHS, the U.S. Coast Guard, U.S. Customs and Border Protection, Transportation Security Administration, U.S. Citizenship and Immigration Services, and U.S. Immigration and Customs Enforcement undertake countless activities to expedite and facilitate the flow of goods and people across U.S. borders. As these agencies have previously done—in some cases for hundreds of years—they ensure seamless integration of these responsibilities with the task of upholding and promoting the security of the country.

\* Today, customs revenue remains second only to internal revenue taxes as the most significant source of Federal revenue, totaling over \$30B annually.

This page intentionally left blank.

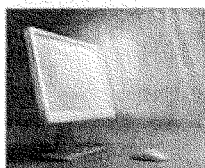
## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS



The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive.



As noted earlier, three key concepts form the foundation of our national homeland security strategy designed to achieve this vision: Security, Resilience, and Customs and Exchange. In turn, these key concepts drive broad areas of activity that the QHSR process defines as homeland security missions. *These missions are enterprise-wide, and not limited to the Department of Homeland Security.* These missions and their associated goals and objectives tell us in detail what it means to prevent, to protect, to respond, and to recover, as well as to build in security, to ensure resilience, and to facilitate customs and exchange. Hundreds of thousands of people from across the Federal Government, State, local, tribal, and territorial governments, the private sector, and other nongovernmental organizations are responsible for executing these missions. These are the people who regularly interact with the public, who are responsible for public safety and security, who own and operate our Nation's critical infrastructures and services, who perform research and develop technology, and who keep watch, prepare for, and respond to emerging threats and disasters. These homeland security professionals must have a clear sense of what it takes to achieve the overarching vision articulated above.



### *The Core Missions*

There are five homeland security missions:

1. Preventing terrorism and enhancing security;
2. Securing and managing our borders;
3. Enforcing and administering our immigration laws;
4. Safeguarding and securing cyberspace; and
5. Ensuring resilience to disasters.

In addition, we must specifically focus on maturing and strengthening the homeland security enterprise itself.

#### **IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS**

For each mission, the following discussion, supported with additional material set forth in Section V, details specific goals and objectives that outline what is required for success. These mission goals and objectives reflect the considered analysis conducted through the QHSR process. This analysis included literature reviews, subject-matter expert consultation, public comment, and testing of conclusions against preliminary analytic models. **Appendix B** provides an overview of the QHSR process. The goals and objectives set the stage for developing and applying risk management tools to establish programmatic priorities, develop more specific performance measures, and pursue greater integrated planning across the homeland security enterprise.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### MISSION 1: PREVENTING TERRORISM AND ENHANCING SECURITY

Preventing a terrorist attack in the United States remains the cornerstone of homeland security. Our vision is a secure and resilient Nation that effectively prevents terrorism in ways that preserve our freedom and prosperity. Achieving this vision requires us to focus on the core goal of preventing terrorist attacks, highlighting the challenges of preventing attacks using chemical, biological, radiological, and nuclear (CBRN) weapons and managing risks to critical infrastructure.

We must be vigilant against the use of terrorist tactics employed by malicious actors seeking to harm the United States. Thus, a key element of preventing terrorism is to understand not only the threat that currently confronts us—for example, the terrorist use of explosives—but also evolving and emerging threats. We must actively monitor those threats and put them in an appropriate context so we can apply the most effective threat mitigation strategies possible, including understanding how best to protect against terrorist capabilities and deter and disrupt operations of those who would use terrorist tactics to advance their aims. We must develop a comprehensive understanding of the threats and malicious actors that have the desire and ability to harm the United States. These include individuals, terrorist organizations, hostile foreign intelligence services, those seeking to proliferate weapons of mass destruction, and criminal enterprises. Beyond these efforts, however, we must also stop the spread of violent extremism. In this regard, it is important that we actively engage communities across the United States.

CBRN weapons, especially high-consequence nuclear and biological weapons, pose a particular challenge to our security. We must anticipate emerging CBRN threats, control both access to and movement of CBRN, and expand and strengthen our capabilities to detect, protect against, and deter hostile use.

In addition, we must effectively manage terrorist-based as well as other risks to critical infrastructure. The security and resilience of the critical systems, services, and resources that sustain our daily lives are vital to ensuring that our Nation continues to prosper and thrive. We must deepen our understanding of the nature of the risks to these infrastructures and effectively prioritize our efforts to reduce vulnerabilities. In addition to protecting infrastructure and critical facilities and

**“We are at war against al-**

**Qaeda, a far-reaching network of violence and hatred that attacked us on 9/11, that killed nearly 3,000 innocent people, and that is plotting to strike us again. And we will do whatever it takes to defeat them.”**

**– President Barack Obama**

#### **IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS**

networks, we must also work to make critical infrastructure resilient, including not only stand-alone facilities, but also interdependent systems and networks within and across critical infrastructure sectors.

Finally, one of America's underlying strengths is the ability of the democratic process to withstand the test of time and persevere regardless of efforts to disrupt it. Ensuring the continuity of government and government operations, and protecting our national leaders, is essential to preserving the framework established in the Constitution.

These mission goals and objectives reflect the continued primary importance placed on preventing terrorism. They also reflect a continuing emphasis regarding CBRN materials and technologies, as well as critical infrastructure and key resources. The mission goals and objectives set forth here reflect the President's emphasis on preventing introduction and use of high-consequence weapons of mass destruction, the continued fight against al-Qaeda, and the imperative to increase not only security but also resilience of America's critical infrastructure and key resources.

As noted earlier, the nature of the homeland security enterprise demands that these goals are executed in the context of extensive collaboration at every level of the homeland security enterprise through cooperation with State, local, tribal, and territorial governments, nongovernmental entities, and the private sector.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### Preventing Terrorism and Enhancing Security Mission Goals and Objectives

**Goal 1.1: Prevent Terrorist Attacks:** Malicious actors are unable to conduct terrorist attacks within the United States.

#### Objectives

- **Understand the threat:** Acquire, analyze, and appropriately share intelligence and other information on current and emerging threats.
- **Deter and disrupt operations:** Deter, detect, and disrupt surveillance, rehearsals, and execution of operations by terrorists and other malicious actors.
- **Protect against terrorist capabilities:** Protect potential targets against the capabilities of terrorists, malicious actors, and their support networks to plan and conduct operations.
- **Stop the spread of violent extremism:** Prevent and deter violent extremism and radicalization that contributes to it.
- **Engage communities:** Increase community participation in efforts to deter terrorists and other malicious actors and mitigate radicalization toward violence.

**Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities:** Malicious actors, including terrorists, are unable to acquire or move dangerous chemical, biological, radiological, and nuclear materials or capabilities within the United States.

#### Objectives

- **Anticipate emerging threats:** Identify and understand potentially dangerous actors, technologies, and materials.
- **Control access to CBRN:** Prevent terrorists and other malicious actors from gaining access to dangerous materials and technologies.
- **Control movement of CBRN:** Prevent the illicit movement of dangerous materials and/or technologies.
- **Protect against hostile use of CBRN:** Identify the presence of and effectively locate, disable, or prevent the hostile use of CBRN.

**Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events:** Key sectors actively work to reduce vulnerability to attack or disruption.

#### Objectives

- **Understand and prioritize risks to critical infrastructure:** Identify, attribute, and evaluate the most dangerous threats to critical infrastructure and those categories of critical infrastructure most at risk.
- **Protect critical infrastructure:** Prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions—including linkages through cyberspace—from attacks or disruption.
- **Make critical infrastructure resilient:** Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.
- **Protect government leaders, facilities, and special events.** Preserve continuity of government and ensure security at events of national significance.



## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### MISSION 2: SECURING AND MANAGING OUR BORDERS

A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders. Secure, well-managed borders must not only protect the United States against threats from abroad; they must also expedite the safe flow of lawful travel and commerce. Achieving this vision requires that we focus on three interrelated goals.

First, we must achieve effective control of the physical borders and approaches to the United States. Achieving this aim means not only that we are able to prevent the illegal entry of inadmissible persons and contraband and the illegal exit of dangerous goods, proceeds of crime, and malicious actors, but also that we can securely expedite the cross-border flow of lawful immigration, travel, and commerce at our borders. Indeed, these “twin goals” mutually reinforce each other. The more we use technology, information, and training to support operations that identify and expedite lawful travel and commerce across our borders, the more officials at the border can focus on the known threats that require more scrutiny. We must and can achieve *both* greater security and greater interchange with the world.

Second, to secure our Nation, we must work together to look beyond our borders to identify and disrupt threats well before they reach our shores. Accordingly, we must work with our international partners and with the private sector to prevent the exploitation of the interconnected trading, transportation, and transactional systems that move people and commerce throughout the global economy and across our borders. At the same time, we must also work with those same partners to ensure the security and resilience of those systems in order to expedite and reduce unnecessary encumbrances to lawful travel and trade that may impair economic vitality. America must remain open for business and exchanges with the world, must remain true to its principles of privacy, civil rights, and civil liberties, and must be welcoming of lawful visitors and immigrants.

Third, achieving this vision also requires disrupting and dismantling transnational criminal and terrorist organizations that smuggle or traffic people, illicit goods, or the proceeds of crime across the U.S. border, and commit violent acts. Transnational criminal and terrorist organizations present a dual threat that must be countered. These organizations seek to exploit lawful movement systems for

**“We will strengthen our defenses, but we will not succumb to a siege**

**mentality** that sacrifices the open society and liberties and values that we cherish as Americans, because great and proud nations don’t hunker down and hide behind walls of suspicious and mistrust. That is exactly what our adversaries want...”

— President Barack Obama

#### IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

harmful or dangerous purposes while also seeking to establish alternative illicit pathways through which people and illegal goods—from narcotics to terrorists to illicit funds to dangerous weaponry—can cross U.S. borders. These organizations may also intend to destabilize governments, commit violence, and intimidate innocent people. In order to secure our homeland, therefore, we must also focus on disrupting and dismantling these organizations that seek to exploit the global trade and travel systems that transcend and permeate our borders.

The inclusion of border security and management in its entirety represents an evolution of thinking in homeland security, beyond simply border security. This approach to border security and management also recognizes that while aviation security, maritime security, and land border security are all critical elements of homeland security, we must consider these elements together as an integrated set of concerns, so as not to allow stovepipes and divisions to develop between our security approaches within each of these domains of activity. Moreover, the three-pronged approach set forth here goes beyond the traditional concern with the border itself. This approach emphasizes securing lawful trade and travel through global movement systems, to prevent actions like the attempted terrorist attack on Flight 253 on December 25, 2009, which used the lawful global travel system as a vector for attack. This approach also focuses on disrupting criminal and terrorist organizations that engage in smuggling and trafficking across the U.S. border. These organizations exploit our lawful trade and travel systems for malicious ends, and create illicit smuggling and trafficking pathways that present a threat to our security and economic well-being.

This three-pronged approach to securing and managing our borders can only be achieved by cooperative efforts among Federal departments and agencies, our international partners, and global transnational private-sector partners to establish secure and resilient global trading, transportation, and transactional systems that facilitate the flow of lawful travel and commerce. This approach also depends on partnerships with Federal, State, local, tribal, territorial, and international law enforcement agencies to share information and conduct coordinated and integrated operations. In working together, we are safer, stronger, and can more effectively achieve our shared vision of secure, well-managed borders that protect our people, expedite lawful travel and commerce, and preserve our freedoms and way of life.

#### IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

##### Securing and Managing Our Borders Mission Goals and Objectives

**Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders:** Prevent the illegal flow of people and goods across U.S. air, land, and sea borders while expediting the safe flow of lawful travel and commerce.

###### Objectives

- **Prevent illegal entry:** Prevent the illegal entry of people, weapons, dangerous goods, and contraband, and protect against cross-border threats to health, food, environment, and agriculture, while facilitating the safe flow of lawful travel and commerce.
- **Prevent illegal export and exit:** Prevent the illegal export of weapons, proceeds of crime, and other dangerous goods, and the exit of malicious actors.

**Goal 2.2: Safeguard Lawful Trade and Travel:** Ensure security and resilience of global movement systems.

###### Objectives

- **Secure key nodes:** Promote the security and resilience of key nodes of transaction and exchange within the global supply chain.
- **Secure conveyances:** Promote the safety, security, and resilience of conveyances in the key global trading and transportation networks.
- **Manage the risk posed by people and goods in transit.**

**Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations:** Disrupt and dismantle transnational organizations that engage in smuggling and trafficking across the U.S. border.

###### Objectives

- **Identify, disrupt, and dismantle transnational criminal and terrorist organizations:** Disrupt transnational criminal or terrorist organizations involved in cross-border smuggling, trafficking, or other cross-border crimes, dismantle their infrastructure, and apprehend their leaders.
- **Disrupt illicit pathways:** Identify, disrupt, and dismantle illicit pathways used by transnational criminal and terrorist organizations.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### MISSION 3: ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

---

Virtually all Americans are affected by our immigration system. A fair and effective immigration system enriches American society, unifies families, and promotes our security. Conversely, persistent problems in immigration policy can consume valuable resources needed to advance other security objectives, undermine confidence in the rule of law, and make it harder to focus on the most dangerous threats facing our country. In short, the success of our Nation's immigration policy plays a critical role in advancing homeland security, and our overall homeland security policy must be implemented in a manner that supports an immigration system that succeeds in advancing American interests.

At the heart of any Nation's immigration regime is the imperative to know who lives and works within its national borders. Immigration policy must deter immigration violations, help eliminate the conditions that foster illegal immigration, and improve system efficiency, fairness, and integrity. This vision reflects an emphasis on both immigration enforcement and immigration services, allowing the government to efficiently facilitate lawful immigration while identifying and removing those who violate our laws. Finally, the integration of lawful immigrant communities into American society is central to establishing a safe and secure homeland where all Americans can thrive. The American tradition of welcoming lawful immigrants is not merely a reflection of America's founding values—it also provides national and community benefits in increased security and prosperity.

Successful immigration management will require a unified approach that employs shared policy and priorities, a common understanding and respect for stakeholder roles, as well as improved sharing of information and analysis. As part of this process, the United States must establish effective laws and policies to govern the immigration system.

The strategic aims and objectives set forth below address the key factors needed to promote legal immigration, combat illegal immigration, and effectively administer and enforce our immigration laws.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### Enforcing and Administering Our Immigration Laws Mission Goals and Objectives

**Goal 3.1: Strengthen and Effectively Administer the Immigration System:** Promote lawful immigration, expedite administration of immigration services, and promote the integration of lawful immigrants into American society.

#### Objectives

- **Promote lawful immigration:** Clearly communicate to the public information on immigration services and procedures.
- **Effectively administer the immigrations services system:** Create a user-friendly system that ensures fair, consistent, and prompt decisions.
- **Promote the integration of lawful immigrants into American society:** Provide leadership, support, and opportunities to immigrants to facilitate their integration into American society and foster community cohesion.

**Goal 3.2: Prevent Unlawful Immigration:** Reduce conditions that encourage foreign nationals to illegally enter and remain in the United States, while identifying and removing those who violate our laws.

#### Objectives

- **Reduce demand:** Eliminate the conditions that encourage illegal employment.
- **Eliminate systemic vulnerabilities:** Prevent fraud, abuse, and exploitation, and eliminate other systemic vulnerabilities that threaten the integrity of the immigration system.
- **Prevent entry or admission:** Prevent entry or admission of criminals, fugitives, other dangerous foreign nationals, and other unauthorized entrants.
- **Arrest, detain, prosecute, and remove:** Arrest, detain, prosecute, and remove criminal, fugitive, dangerous, and other unauthorized foreign nationals consistent with due process and civil rights protections.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### MISSION 4: SAFEGUARDING AND SECURING CYBERSPACE

---

Our economic vitality and national security depend today on a vast array of interdependent and critical networks, systems, services, and resources. We know this interconnected world as *cyberspace*, and without it we cannot communicate, travel, power our homes, run our economy, or obtain government services. Its benefits are tremendous.

Yet as we migrate ever more of our economic and societal transactions to cyberspace, these benefits come with increasing risk. Not only is cyberspace inherently insecure as built, but as a Nation we face a variety of adversaries who are working day and night to use our dependence on cyberspace against us. Sophisticated cyber criminals and nation-states, among others, are among the actors in cyberspace who now pose great cost and risk both to our economy and national security. They exploit vulnerabilities in cyberspace to steal money and information, and to destroy, disrupt, or threaten the delivery of critical services.

For this reason, safeguarding and securing cyberspace has become one of the homeland security community's most important missions. Our vision is a cyberspace that supports a secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.

We will achieve this vision by focusing on two goals: (1) helping to create a safe, secure, and resilient cyber environment; and (2) promoting cybersecurity knowledge and innovation. We must enhance public awareness and ensure that the public both recognizes cybersecurity challenges and is empowered to address them. We must create a dynamic cyber workforce across government with sufficient capacity and expertise to manage current and emerging risks. We must invest in the innovative technologies, techniques, and procedures necessary to sustain a safe, secure, and resilient cyber environment. Government must work creatively and collaboratively with the private sector to identify solutions that take into account both public and private interests, and the private sector and academia must be fully empowered to see and solve ever larger parts of the problem set. Finally, because cybersecurity is an exceedingly dynamic field, we must make specific efforts to ensure that the Nation is prepared for the cyber threats and challenges of tomorrow, not only of today. To do this, we must promote cybersecurity knowledge and innovation. Innovation in technology, practice, and policy must further protect—not erode—privacy and civil liberties.

#### IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

##### Safeguarding and Securing Cyberspace Mission Goals and Objectives

**Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment:** Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure.

###### Objectives

- **Understand and prioritize cyber threats:** Identify and evaluate the most dangerous threats to Federal civilian and private-sector networks and the Nation.
- **Manage risks to cyberspace:** Protect and make resilient information systems, networks, and personal and sensitive data.
- **Prevent cyber crime and other malicious uses of cyberspace:** Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.
- **Develop a robust public-private cyber incident response capability:** Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.

**Goal 4.2: Promote Cybersecurity Knowledge and Innovation:** Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.

###### Objectives

- **Enhance public awareness:** Ensure that the public recognizes cybersecurity challenges and is empowered to address them.
- **Foster a dynamic workforce:** Develop the national knowledge base and human capital capabilities to enable success against current and future threats.
- **Invest in innovative technologies, techniques, and procedures:** Create and enhance science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### MISSION 5: ENSURING RESILIENCE TO DISASTERS

---

Despite ongoing vigilance and efforts to protect this country and its citizens, major accidents and disasters, as well as deliberate attacks, will occur. The challenge is to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises. Our vision is a Nation that understands the hazards and risks we face; is prepared for disasters; can withstand the disruptions disasters may cause; can sustain social trust, economic, and other functions under adverse conditions; can manage itself effectively during a crisis; can recover quickly and effectively; and can adapt to conditions that have changed as a result of the event.

The strategic aims and objectives for this mission are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements create the resilience to disasters so necessary to the functioning and prosperity of this Nation.

Achieving resilience will require a significant change in U.S. emergency management from a primary focus on response and recovery to one that takes a wider view, balancing response and recovery with mitigation and preparedness. In addition, we must more fully incorporate a comprehensive understanding of risk to establish priorities and inform decisionmaking. Resilience will also require a shift from a reliance on top-down emergency management to a process that engages all stakeholders—local, tribal, territorial, and State governments, Federal departments and agencies, as well as nongovernmental organizations, the private sector, and individuals, families, and communities.

Disasters, by their very nature, occur locally—in communities very often far removed from Federal assets. The elements of the homeland security enterprise geared toward responding to disasters are thus widely distributed. Experience shows that the first line of defense rests with individuals, families, and communities, who must take responsibility for their own safety and must be prepared to respond to and possibly endure a crisis when disaster strikes. State, local, territorial, and tribal responders will usually be the first official presence on the scene, while the Federal Government will provide support when effective response exceeds their capabilities. Nongovernmental organizations are also key partners and provide essential humanitarian and relief services, while the private sector is responsible for the economic welfare of areas affected by disasters and for much of the Nation's critical infrastructure.

Disasters such as 9/11 and Hurricane Katrina have demonstrated that despite occurring in specific locations, catastrophes have national consequences whose burdens we all share. Disasters have also illustrated the ability and importance of



#### **IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS**

communities to come together to help one another through difficult times and of effective information sharing and situational awareness. The strategic aims and objectives for this mission reinforce the importance of the traditional emergency management activities—preparing individuals, communities, organizations, and governments to be able to respond to and recover from all threats and hazards— but also advance the importance of taking a more holistic approach when considering these activities to ensure greater resilience in our communities and for our Nation.

#### IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

##### Ensuring Resilience to Disasters Mission Goals and Objectives

**Goal 5.1: Mitigate Hazards:** Strengthen capacity at all levels of society to withstand threats and hazards.

###### Objectives

- **Reduce the vulnerability of individuals and families:** Improve individual and family capacity to reduce vulnerabilities and withstand disasters.
- **Mitigate risks to communities:** Improve community capacity to withstand disasters by mitigating known and anticipated hazards.

**Goal 5.2: Enhance Preparedness:** Engage all levels and segments of society in improving preparedness.

###### Objectives

- **Improve individual, family, and community preparedness:** Ensure individual, family, and community planning, readiness, and capacity-building for disasters.
- **Strengthen capabilities:** Enhance and sustain nationwide disaster preparedness capabilities, to include life safety, law enforcement, information sharing, mass evacuation and shelter-in-place, public health, mass care, and public works.

**Goal 5.3: Ensure Effective Emergency Response:** Strengthen response capacity nationwide.

###### Objectives

- **Provide timely and accurate information to the public:** Establish and strengthen pathways for clear, reliable, and current emergency information, including effective use of new media.
- **Conduct effective disaster response operations:** Respond to disasters in an effective and unified manner.
- **Provide timely and appropriate disaster assistance:** Improve governmental, nongovernmental, and private-sector delivery of disaster assistance.

**Goal 5.4: Rapidly Recover:** Improve the Nation's ability to adapt and rapidly recover.

###### Objectives

- **Enhance recovery capabilities:** Establish and maintain nationwide capabilities for recovery from major disasters.
- **Ensure continuity of essential services and functions:** Improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions.

## IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

### MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

---

This QHSR has drawn on our Nation's experience in the years since 9/11 to highlight the importance of joining efforts across all levels of society and government in a common homeland security enterprise. Looking forward, and as we consider the evolution of homeland security and this enterprise, we recognize that the enterprise itself requires active stewardship. In this regard, we have identified several key areas for strengthening: shared awareness of risks and threats; community capability and readiness; unity of effort across all participants in the homeland security enterprise; and innovation through active application of leading-edge science and technology.

The effort to strengthen the homeland security enterprise must begin with an evolution in how we think about homeland security itself. All of the most advanced, high-tech tools in the world will not transform our security unless we change our way of thinking, the way we approach individual, family, and community preparedness, the way we organize, train, and equip our professional capabilities, and the way all of these elements interact. Today, we must counter myriad threats that range from hostile aircraft entering our airspace to people carrying backpacks to suspicious packages left on subways. For other hazards—major accidents, natural disasters—we must be better able to respond to crises, while recognizing that the Federal Government will not always serve as the primary lead. We must also find better ways to mitigate common hazards and reduce systemic vulnerabilities.

We must shorten the cycles of identifying possible threats to addressing them—whether by interdicting hostile actors, stopping dangerous cargoes, or detecting releases of deadly chemical or biological weapons and quickly providing antidotes or treatments. This means building greater real-time, shared threat information analysis and situational awareness. It means aggressively identifying, countering, and defeating hostile intelligence activities against the homeland. It also means building stronger, more capable communities to address threats before they manifest themselves and to shorten the crisis-to-care timelines following a disaster.

We must avoid stovepipes that hinder appropriate information sharing and analysis, and we must foster greater information sharing without undermining privacy protections or civil liberties. Moving from a top-down, command and control model to a more bottom-up approach in homeland security will require greater dynamic coordination—where individuals, communities, and other stakeholders at all levels understand their roles and are empowered with information, resources, and the capability to be part of our national effort to protect ourselves.

#### **IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS**

We must also strengthen communities so that they have the information, training, and equipment they need to respond effectively in the immediate face of a warning or crisis event. Creating capable communities will require that we establish clear standards for readiness, promulgate accurate and timely information to communicate risks, make opportunities for training, education, and exercises available, and ensure that critical capabilities—such as effective interoperable communications—are in place and functional. Achieving this goal will demand active partnering among all levels of government.

In addition, there is a need to enhance the skills and abilities of homeland security professionals as part of the larger national security professional development effort, expand the partnerships upon which the homeland security enterprise depends, develop technologies that support the achievement of homeland security mission goals and objectives, and institutionalize processes that will support effective and informed decisionmaking and unity of effort within the enterprise. Each of these aims strengthens decisionmaking, identification of priorities, and successful execution of the homeland security missions.

The strategic aims and objectives for maturing and strengthening the homeland security enterprise are drawn from the common themes that emerge from each of the homeland security mission areas. Ensuring shared awareness of risks and threats, building capable communities, creating unity of effort, and enhancing the use of science and technology underpin our national efforts to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters.

#### IV. OVERVIEW OF THE HOMELAND SECURITY MISSIONS

##### Maturing and Strengthening the Homeland Security Enterprise Goals and Objectives

**Enhance Shared Awareness of Risks and Threats:** Establish a comprehensive system for building and sharing awareness of risks and threats.

**Objectives**

- **Establish an approach to national-level homeland security risk assessments:** Develop and implement a methodology to conduct national-level homeland security risk assessments.
- **Share information and analysis:** Enhance critical tools and institutionalize arrangements for effective, timely sharing of information and analysis.
- **Screen and verify identity:** Establish a robust approach to identity verification that safeguards individual privacy and civil rights.
- **Enhance domain awareness:** Ensure shared situational awareness in the air, land, and maritime domains.
- **Integrate counterintelligence:** Use and integrate counterintelligence in all aspects of homeland security to thwart attacks against the homeland.
- **Establish a common security mindset:** Promote a common understanding of security and threat awareness as a shared responsibility.

**Build Capable Communities:** Foster communities that have information, capabilities, and resources to prevent threats, respond to disruptions, and ensure their own well-being.

**Objectives**

- **Set capability and capacity standards:** Identify core capability and capacity targets to guide homeland security investments and activities across the enterprise.
- **Enhance systems for training, exercising, and evaluating capabilities.**
- **Maintain and sustain equipment and capabilities:** Promote smart investment in operational capabilities.

**Foster Unity of Effort:** Foster a broad national culture of cooperation and mutual aid.

**Objectives**

- **Build a homeland security professional discipline:** Develop the homeland security community of interest at all levels of government as part of a cadre of national security professionals.
- **Promote regional response capacity:** Promote mutual aid agreements for response requirements that exceed local capacity.
- **Institutionalize homeland security planning:** Develop a planning system to execute homeland security activities.
- **Further enhance the military-homeland security relationship:** Strengthen unity of effort between military and civilian activities for homeland security.
- **Strengthen the ability of Federal departments and agencies to support homeland security missions**
- **Expand and extend governmental and private sector international partnerships:** Transform how government and the private sector interact.
- **Mature the Department of Homeland Security:** Improve DHS's organizational and programmatic alignment and its management systems and processes.

**Foster Innovative Approaches and Solutions Through Leading-Edge Science and Technology:** Ensure scientifically informed analysis and decisions are coupled to innovative and effective technological solutions.

**Objectives**

- **Scientifically study threats and vulnerabilities:** Pursue a rigorous scientific understanding of current and future threats to homeland security and the possible means to their prevention and mitigation.
- **Develop innovative approaches and effective solutions:** Encourage and enable innovative approaches to critical homeland security challenges, fostering collaborative efforts involving government, academia, and the private sector.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

This section elaborates the goals and objectives for each of the five homeland security missions, as well as for maturing and strengthening the homeland security enterprise. As noted above, these missions and their associated goals and objectives tell us in detail what it means to prevent, to protect, to respond, and to recover, as well as to build in security, to ensure resilience, and to facilitate customs and exchange. These missions are enterprise-wide, and not limited to the Department of Homeland Security. Five selected strategic outcomes are identified for each mission, along with key actions for each of the mission objectives.

### **Mission 1: Preventing Terrorism and Enhancing Security**

- Goal 1.1: Prevent Terrorist Attacks
- Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities
- Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events

### **Mission 2: Securing and Managing Our Borders**

- Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders
- Goal 2.2: Safeguard Lawful Trade and Travel
- Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

### **Mission 3: Enforcing and Administering Our Immigration Laws**

- Goal 3.1: Strengthen and Effectively Administer the Immigration System
- Goal 3.2: Prevent Unlawful Immigration

### **Mission 4: Safeguarding and Securing Cyberspace**

- Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment
- Goal 4.2: Promote Cybersecurity Knowledge and Innovation

### **Mission 5: Ensuring Resilience to Disasters**

- Goal 5.1: Mitigate Hazards
- Goal 5.2: Enhance Preparedness
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Rapidly Recover

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### MISSION 1: PREVENTING TERRORISM AND ENHANCING SECURITY

Preventing terrorism in the United States is the cornerstone of homeland security. Ensuring that malicious actors cannot conduct terrorist attacks within the United States, preventing the illicit or hostile use of chemical, biological, radiological, and nuclear (CBRN) materials or capabilities within the United States, and managing risks to our critical infrastructure and key resources helps us realize our vision of a secure and resilient Nation.

#### Key Strategic Outcomes

- Acts of terrorism against transportation systems are thwarted prior to successful execution.
- The manufacture, storage, or transfer of dangerous materials is protected by physical, personnel, and cybersecurity measures commensurate with the risks.
- Any release of high-consequence biological weapons is detected in time to protect populations at risk from the release.
- Critical infrastructure sectors adopt and sector partners meet accepted standards that measurably reduce the risk of disrupting public health and safety, critical government services, and essential economic activities.
- Governmental executive leadership is protected from hostile acts by terrorists and other malicious actors.

#### Goal 1.1: Prevent Terrorist Attacks

**Malicious actors are unable to conduct terrorist attacks within the United States.** Success in achieving this goal rests on our ability to strengthen public- and private-sector activities designed to counter terrorist efforts to plan and conduct attacks. Success also depends on strengthening our ability to investigate and arrest perpetrators of terrorist crimes and to collect intelligence that will help prevent future terrorist activities.

#### Objectives

- **Understand the threat:** Acquire, analyze, and appropriately share intelligence and other information on current and emerging threats. Homeland security partners require a shared understanding of the current and emerging threats from terrorists and other malicious actors to inform the development of risk management strategies. As has long been recognized, information and intelligence regarding emerging threats must be collected.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

analyzed, and disseminated appropriately and promptly. Homeland security partners must use compatible information architecture and data standards where possible to maximize the acquisition, access, retention, production, use, management, and appropriate safeguarding of this information.

- **Deter and disrupt operations:** Deter, detect, and disrupt surveillance, rehearsals, and execution of operations by terrorists and other malicious actors. We must deter and disrupt malicious actors and dismantle support networks at every step of their operations. This objective also includes identifying and disrupting efforts to corrupt cyber or movement systems, breach confidentiality, or deny authorized access. Prompt and appropriate law enforcement and legal action against perpetrators and dismantling of their support networks will mitigate hostile actions.
- **Protect against terrorist capabilities:** Protect potential targets against the capabilities of terrorists, malicious actors, and their support networks to plan and conduct operations. We must be able to protect against the capabilities that malicious actors might use to conduct terrorism against the United States. This objective includes detecting, disrupting, and preventing the ability of malicious actors intent on using terrorism to train, plan, travel, finance their operations, communicate, and acquire weapons—including high-yield explosives. We must protect against the full range of these capabilities in order to reduce the likelihood of a successful attack against the United States.
- **Stop the spread of violent extremism:** Prevent and deter violent extremism and radicalization that contributes to it. Reducing violent extremism will frustrate terrorist efforts to recruit operatives, finance activities, and incite violence. In particular, efforts must focus not only at the community level, but also on cyberspace.
- **Engage communities:** Increase community participation in efforts to deter terrorists and other malicious actors and mitigate radicalization toward violence. Individual citizens and cohesive communities are key partners in the homeland security enterprise and have an essential role to play in countering terrorism. Mechanisms for identifying and reporting suspicious activities must be made clear and accessible. Moreover, enhanced public preparedness and effective warning systems can empower communities, help minimize fear, and diminish the effectiveness of terrorist tactics.



## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

---

### Goal 1.2: Prevent the Unauthorized Acquisition or Use of CBRN Materials and Capabilities

---

Malicious actors, including terrorists, are unable to acquire or move dangerous chemical, biological, radiological, and nuclear materials or capabilities within the United States. Although the Nation remains committed to preventing all attacks by terrorists and other malicious actors, certain chemical, biological, radiological, and nuclear attacks pose a far greater potential to cause catastrophic consequences. Consequently, particular attention must be paid to the security of dangerous chemical, biological, radiological, and nuclear materials and technologies.

#### Objectives

- **Anticipate emerging threats: Identify and understand potentially dangerous actors, technologies, and materials.** It is incumbent upon us to identify changing capabilities *before* their first use so that appropriate risk management strategies can be developed and executed. Homeland security partners must identify, characterize, and have timely and appropriate information and analysis on emerging and potentially dangerous technologies and materials. Information and analysis on emerging threats must be appropriately and effectively shared among homeland security partners.
- **Control access to CBRN: Prevent terrorists and other malicious actors from gaining access to dangerous materials and technologies.** American industry transforms raw materials and technologies into economic progress, but in the wrong hands, such materials and capabilities pose critical threats to public health and safety. Controlling access to CBRN materials and technologies is an essential step in preventing their illicit use. Access to these materials and technologies must be limited to legitimate users. Industries that manufacture, store, or sell potentially dangerous materials, and experts with knowledge of their use, must maintain awareness of the status of CBRN materials and technologies and assume responsibility for their security and control. Personnel surety programs must be strengthened. Finally, the manufacturing, storage, and transfer of dangerous materials must be protected by physical and cybersecurity measures commensurate with the risks they pose.
- **Control movement of CBRN: Prevent the illicit movement of dangerous materials and technologies.** Should malicious actors obtain CBRN, attacks can be prevented or deterred if movement of CBRN is more effectively controlled. Differentiating between the licit and illicit movement of dangerous materials and technologies will require the cooperation of public- and private-sector homeland

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

security enterprise partners to ensure such materials and technologies are secure and accounted for, and their movement is known to appropriate authorities. Terrorists and other malicious actors must be impeded in their ability to move dangerous materials, technologies, and expertise into, within, or out of the United States through appropriate screening, detection, and inspection regimes, and through efforts to prevent the financing of their activities.

- **Protect against hostile use of CBRN:** Identify the presence of and effectively locate, disable, or prevent the hostile use of CBRN. Measures must be in place to discover the presence of CBRN, as well as to rapidly apply the technology and expertise necessary to locate, disable, or otherwise prevent use of CBRN weapons.

---

### Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events

---

Key sectors actively work to reduce vulnerability to attack or disruption. The American way of life depends upon the effective functioning of the Nation's critical infrastructure and key resources, and the protection of key leadership and events. Although considerable advances have been made in identifying critical infrastructure assets and systems, and understanding the current, emerging, and future risks to those infrastructures, the breadth of the infrastructure, its increasing reliance on cyberspace, and its criticality necessitates continued diligence.

#### Objectives

- **Understand and prioritize risks to critical infrastructure:** Identify, attribute, and evaluate the most dangerous threats to critical infrastructure and those categories of critical infrastructure most at risk. Homeland security partners and stakeholders need a shared understanding of the risks to and the interdependencies that connect the Nation's critical

**Homeland security includes the unique responsibility of protecting the President of the United States**, the Vice President, visiting heads of state, and the Presidential campaign process, as well as ensuring the continuity of national leadership. At the Federal level, the U.S. Secret Service assumed this responsibility after the assassination of President William McKinley in 1901. At the State, local, tribal, and territorial levels, law enforcement agencies and protective services provide similar functions.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

infrastructure and key resources. Homeland security partners must provide and receive information and assessments on current and emerging risks in time to carry out their risk management responsibilities, while enjoying access to the data, tools, and expertise to make informed risk management decisions. Acquisition, access, retention, production, use, and management of threat and risk information must be maximized through compatible information architecture and data standards. Risk management decisions made by homeland security partners must account for interdependencies across sectors and jurisdictions.

- **Protect critical infrastructure: Prevent high-consequence events by securing critical infrastructure assets, systems, networks, or functions—including linkages through cyberspace—from attacks or disruption.**

Homeland security partners must be aware of the risk profiles of and risk management strategies for critical infrastructure, to include key governmental sites that have national symbolic importance as well as serve as vital functions to our democratic institutions. Measures to control, and in some cases deny, access to critical infrastructure assets, systems, and networks must be consistently implemented, upgraded, and enforced. These measures must also continuously adapt based on an improved understanding of changing threats and risks. Additionally, business processes and infrastructure operations must be changed or revised and technologies incorporated to reduce the risk of high-consequence events.
- **Make critical infrastructure resilient: Enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.**

The Nation cannot rely on protection strategies alone to ensure the continuity of critical functions, particularly those necessary for public health and safety. Homeland security partners must develop, promulgate, and update guidelines, codes, rules, regulations, and accepted standards when appropriate, that measurably reduce the risk of damage and disruption to critical functions, networks, and systems, and ensure their resilience. Design of new infrastructure and infrastructure improvements must anticipate change in the risk environment, incorporate lessons from past events and exercises, and consider and build in security and resilience from the start. Finally, a skilled workforce with sufficient capacity and expertise is necessary in order to ensure the functionality of critical infrastructure.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

- **Protect governmental leaders, facilities, and special events:** Preserve continuity of government and ensure security at events of national significance. Preserving continuity of government is essential to the stability of the Nation. Detecting, disrupting, and responding to crises under any contingency requires collaboration throughout the homeland security enterprise. Identifying, analyzing, and disseminating protective intelligence information pertaining to individuals, groups, and technologies that pose a danger to our Nation's leadership and visiting heads of state and government is imperative to safeguarding our Nation's interests. So too is actual protection of government facilities. In addition, Federal, State, local, tribal, and territorial homeland security partners execute operational security plans that ensure the safety of American citizens at events of national significance. Homeland security stakeholders play a critical role in the execution of layered security measures to address the threat spectrum. Developing and fostering critical coalitions such as task forces, fusion centers, and working groups reinforces strategic investigative alliances, aids in identifying patterns and trends, and allows sharing of emerging technologies, systems, and methodologies.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### MISSION 2: SECURING AND MANAGING OUR BORDERS

A safe and secure homeland requires that we maintain effective control of our air, land, and sea borders; that we safeguard lawful trade and travel; and that we disrupt transnational organizations that engage in smuggling and trafficking across the U.S. border. This three-pronged approach to securing and managing our borders can only be achieved by working with partners from across the homeland security enterprise to establish secure and resilient global trading, transportation, and transactional systems that facilitate the flow of lawful travel and commerce. This approach also depends on partnerships with Federal, State, local, tribal, territorial, and international law enforcement agencies to share information and conduct coordinated and integrated operations. In working together, we can more effectively achieve our shared vision and preserve our freedoms and way of life.

#### Key Strategic Outcomes

- The entry or approach of all high-consequence WMD and related materials and technologies is prevented.
- Terrorists and other high-risk individuals are prevented from using commercial or noncommercial transportation destined for the United States.
- The identity of all individuals who are encountered at U.S. borders and in global movement systems entering the United States is verified.
- Individuals with known ties to terrorism or transnational criminal activities are not granted access to secure areas within the global movement system.
- No highly dangerous pathogens or organisms are introduced across U.S. borders.

#### Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders

**Prevent the illegal flow of people and goods across U.S. air, land, and sea borders while expediting the safe flow of lawful travel and commerce.** Key to achieving secure and well-managed borders are the broad legal authorities utilized by trained officers to conduct appropriate searches, seizures, arrests, and other key enforcement activities. These security and enforcement activities are balanced, however, by the need to facilitate the lawful transit of people and goods across our borders. Through the collection, analysis, and proper sharing of information, the use of screening and identification verification techniques, the employment of advanced detection and other technologies, the use of "trusted traveler" or "trusted shipper" approaches, and cooperation with our international partners and the private sector,

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

we can achieve security at our borders, enforce the laws, and ensure our prosperity and freedom by speeding lawful travel and commerce.

### Objectives

- **Prevent illegal entry:** Prevent the illegal entry of people, weapons, dangerous goods, and contraband, and protect against cross-border threats to health, food, environment, and agriculture, while facilitating the safe flow of lawful travel and commerce. Central to the mission of controlling our borders is preventing the illegal entry of dangerous persons, contraband, or other illicit goods—whether they are terrorists, highly dangerous weapons, illicit drugs, dangerous pathogens, invasive species, or counterfeit software. Preventing illegal entry must be accomplished both at official ports of entry—in concert with facilitating the safe flow of lawful travel and commerce—and in the long stretches between these points, as well as along our maritime borders and across our air boundaries. We must substantially increase situational awareness at our borders and approaches in order to help detect and classify potential threats and effectively resolve them. We must positively identify individuals encountered to determine their risk to the country, and expedite the collection, sharing, and analysis of all relevant information so that border officers can make accurate security determinations, reduce unknowns in the system, and expedite low-risk individuals and commerce. We must enhance measures aimed at deterring illegal migration and contraband smuggling, thereby reducing “pull” factors that draw unlawful migrants and dangerous goods. Finally, we must build on our existing partnerships with our North American neighbors in order to collaboratively address threats to the continent and approaches and more effectively expedite and secure the lawful flow of travel and commerce within the North American community.
- **Prevent illegal export and exit:** Prevent the illegal export of weapons, proceeds of crime, and other dangerous goods, and the exit of malicious actors. Gaining control of the borders also means gaining better control of what leaves our country. Indeed, violent international drug trafficking organizations are fueled by the proceeds of drug sales smuggled out of the United States, and armed by weapons, some of which are obtained in this country and smuggled across our borders. Hostile and criminal actors seek to smuggle weapons, weapons components, bulk cash, and controlled technologies out of the United States, as well as seek U.S.-based financing for their activities. To address these threats, relevant authorities must identify and assess the risk of all commercial cargo exiting the United States through official channels, and known or suspected terrorists or criminals must be prevented from departing the United

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

States. Additionally, outbound smuggling must be reduced through collaboration with international and private-sector partners, both at home and overseas. Finally, authorities throughout the homeland security enterprise must identify, share, and act upon information to prevent all known or suspected terrorists and wanted criminals from leaving the United States or seeking to enter neighboring countries.

---

### Goal 2.2: Safeguard Lawful Trade and Travel

---

**Ensure security and resilience of global movement systems.** The global economy is increasingly a seamless economic environment connected by systems and networks that transcend national boundaries. The United States is deeply linked to other countries through the flow of goods and services, capital and labor, and information and technology into and across our borders. As much as these global systems and networks are critical to the United States and our prosperity, their effectiveness and efficiency also make them attractive targets for exploitation by our adversaries, terrorists, and criminals. Thus, border security cannot begin simply at our borders. The earlier we can identify, understand, interdict, and disrupt plots and illegal operations, the safer we will be at home. In other words, our borders should not be our first line of defense against global threats. This premise demands a focus on using our national leverage to build partnerships to secure key nodes and conveyances in the global trading and transportation networks, as well as to manage the risks posed by people and goods in transit. Moreover, U.S. national interests—in a competitive U.S. economy and a stable global trading system—require us to work with international partners and the private sector to secure global movement systems. These same national interests are also served by ensuring the free, lawful movement of people and commerce through the global economy and across U.S. borders in a manner that does not impair economic vitality, while at the same time safeguarding privacy, civil rights, and civil liberties.

#### Objectives

- **Secure key nodes: Promote the security and resilience of key nodes of transaction and exchange within the global supply chain.** A variety of actors are involved in the complex process of moving goods and people through the global supply chain from origin to final destination. Each nodal transfer—such as from one international airport or seaport to another, or from one entity to the next—presents adversaries with a new opportunity to introduce a threat into the global supply chain or exploit this system for their own purposes. These key nodes and exchange points must be secured from threats and made able to withstand disruption. In addition, advance information and sophisticated

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

analytic capabilities must be used to reduce unknowns in the system, so that interventions can focus on identified threats or higher risks. Finally, the U.S. Government must work with its international partners and the private sector to build on existing efforts to develop, strengthen, and implement international standards for securing the key systems of the global economy and more effectively facilitating the flow of lawful travel and commerce throughout the world and across U.S. borders.

- **Secure conveyances: Promote the security and resilience of conveyances in the key global trading and transportation networks.** A key component of global movement systems are the conveyances—the forms of transit used to move people and goods from a point of origin toward a final destination—and the operators in that system, including air carriers, cruise ship operators, exporters, cargo carriers, importers, manufacturers, and longshoremen, among others. Operators and the conveyances used to move people and goods from an origin toward a final destination must be identified and determined not to pose a threat to the United States or the larger global movement system. In addition, operators must ensure against the misuse of equipment or transportation that would allow for the introduction of dangerous or illegal contents into the system. Finally, conveyances or shipments approaching or entering the United States through a port of entry must be assessed to determine if they may legally enter the United States or whether they should be subject to additional inspection, if deemed a potential threat or if authorities otherwise believe appropriate.
- **Manage the risk posed by people and goods in transit.** People seeking to come to the United States, as well as goods in transit, must be positively identified and determined not to pose a threat to this country or the larger global movement system as far in advance as possible. For movement of people, this assessment can be performed early through visa processes, online application for travel authorization, and advance provision of passenger biographical information, in order to expedite the flow of international travel. For movement of goods, the assessment is ideally done well before shipment to the United States, or even earlier in the supply chain, in conjunction with private-sector entities and international partners. Identifying people and goods that pose minimal risk as early in the process as possible and securely expediting their travel to and through the United States also facilitates the flow of lawful travel and commerce and reduces friction in the global economy. Supporting networks to share information and analysis regarding people and goods must be robust and effective while protecting privacy and civil liberties. Enhanced global



## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

standards for information collection and sharing increase the effectiveness of these risk assessment efforts. These activities are key to ensuring the safe, lawful flow of commerce, reducing processing times for individuals and goods seeking lawful entry to the country, and ensuring that the United States remains open for business to the world and welcoming of international visitors.

---

### Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations

---

**Disrupt and dismantle transnational organizations that engage in smuggling and trafficking across the U.S. border.** We have also learned in the years since 9/11 that it is not enough to simply interdict trouble at the border or enhance the protection of global systems for trade and travel. Criminals, terrorist networks, and other malicious actors will seek to exploit the same interconnected systems and networks of the global economy for nefarious purposes, or create their own illicit pathways for smuggling and trafficking—of illegal drugs, illegal migrants, terrorists, or even highly dangerous weapons. When these organizations or actors are successful, they also may increase corruption and engage in a wide variety of other criminal activities such as money laundering, bulk cash smuggling, and intellectual property crime, which threaten the rule of law, potentially endanger lives, and generate wider destabilization. Thus, our border strategy must also focus on reducing the power and capability of these transnational criminal and terrorist organizations.

#### Objectives

- **Identify, disrupt, and dismantle transnational criminal and terrorist organizations:** Disrupt transnational criminal or terrorist organizations involved in cross-border smuggling, trafficking, or other cross-border crimes, dismantle their infrastructure, and apprehend their leaders. Identifying, disrupting, and dismantling criminal and terrorist organizations transcends any one Federal agency, State, local, tribal, or territorial law enforcement agency, or Intelligence Community partner. Success will require many key activities. First, all relevant information held by authorities concerning known or suspected terrorists, criminals, illicit organizations and networks, and inadmissible foreign nationals must be appropriately shared among agencies so malicious actors are interdicted by authorities. Working together, the operations of the major transnational criminal and terrorist organizations must be disrupted, and supporting organizations, networks, and infrastructure must be substantially dismantled. The leaders of these organizations must be apprehended and brought to justice.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

- **Disrupt illicit pathways:** Identify, disrupt, and dismantle illicit pathways used by criminal and terrorist organizations. In addition to exploiting lawful systems for global travel and trade, criminal and terrorist organizations create their own illegal pathways for smuggling and trafficking people and goods across international borders. While these routes and conveyances may be used today to transport illicit narcotics or facilitate illegal migration, the same routes may also be used to smuggle terrorists and their tools and finances, or even highly dangerous weapons and materials. Working appropriately with domestic law enforcement partners, the Intelligence Community, and foreign partners, we must identify these illicit pathways, understand their nodes and conveyances, monitor their use, and effectively intervene to stop dangerous people or goods in transit and dismantle the pathways themselves.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### MISSION 3: ENFORCING AND ADMINISTERING OUR IMMIGRATION LAWS

A fair and effective immigration system must protect the public while also enriching American society and promoting economic prosperity. At the same time, it must also deter immigration violations, work to eliminate the conditions that foster illegal immigration, and improve the efficiency, fairness, and integrity of our immigration system.

#### Key Strategic Outcomes

- The identities of individuals seeking immigration services are verified at first contact and throughout the immigration process.
- All workers are verified as legally authorized to work in the United States.
- Real-time information, data, trends, and intelligence on terrorist or criminal organizations and individuals are accessible to all Federal immigration partners.
- Criminal organizations and individuals are prevented from transporting, housing, or harboring illegal aliens.
- All communities that are home to immigrant populations have programs that effectively integrate immigrants into American civic society.

#### Goal 3.1: Strengthen and Effectively Administer the Immigration System

**Promote lawful immigration, expedite administration of immigration services, and promote the integration of lawful immigrants into American society.** Effective administration of the immigration system depends on ensuring that immigration decisions are fair, lawful, and sound; that the immigration system is interactive and user friendly; that policy and procedural gaps are systematically identified and corrected; and that vulnerabilities that would allow persons to exploit the system are eliminated. In addition, effectively administering the immigration system includes efforts to integrate lawful immigrants into American society.

#### Objectives

- **Promote lawful immigration:** Clearly communicate with the public about immigration services and procedures. Lawful immigration contributed greatly to the building of America and continues to enrich our society, our economy, and our way of life. Promoting lawful immigration requires transparent procedures and sustained efforts to inform the public about immigration programs and policies. Thus, to promote lawful immigration, all

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

appropriate information regarding immigration programs, eligibility requirements, application instructions, and status updates must be available to external users through multiple user-friendly avenues, including an interactive, Web-based portal. Feedback from stakeholders must be obtained and assessed in an integrated manner, and solutions, current policies, and policy changes must be clearly communicated to stakeholders and to the public.

- **Effectively administer the immigration services system:** Create a user-friendly system that ensures fair, consistent, and prompt decisions. Applications for immigration services must be efficiently and effectively received and managed. All information needed to make immigration decisions must be available to appropriate agencies electronically and in real-time, including active individual case files and biometric information. In addition, gaps and inconsistencies in policies and procedures must be identified and corrected, while policy guidance must be effectively communicated to the field. Finally, policy implementation must be evaluated to ensure compliance and consistency in the field.
- **Promote the integration of lawful immigrants into American society:** Provide leadership, support, and opportunities to lawful immigrants to facilitate their integration into American society and foster community cohesion. Homeland security partners and stakeholders must work collectively to provide strategies that respect newcomers while encouraging and assisting eligible immigrants to naturalize. Communities that are home to lawful immigrants must have the necessary tools to engage lawful immigrants in civic activities and community issues. New lawful immigrant communities should be encouraged to become an integral part of American life. For their part, new lawful immigrants must obey all applicable laws and take affirmative steps to fully join their new society. This includes learning English and the civic principles that form the foundation of responsible citizenship.

### Promoting integration

reinforces a resilient public where all people belong, are secure in their rights, are confident to exercise their civil liberties, and have opportunities to be full participants in America. The integration process ensures a stronger and more cohesive American society by inviting newcomers from every background to share in our core beliefs and be able to embrace the rights and responsibilities of citizenship.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

---

### Goal 3.2: Prevent Unlawful Immigration

---

**Reduce conditions that encourage foreign nationals to illegally enter and remain in the United States, while identifying and removing those who violate our laws.** To prevent illegal immigration, all agencies charged with immigration administration and enforcement activities must address conditions and factors that create incentives for those illegally entering and staying within the United States. This effort includes identifying the conditions and addressing gaps in current laws, policies, and procedures that foster illegal immigration. Enforcement efforts must prioritize the identification and removal of dangerous foreign nationals who threaten our national security or the safety of our communities and must include safe and humane detention conditions and respect for due process and civil rights as accorded by law.

#### Objectives

- **Reduce demand:** **Eliminate the conditions that encourage illegal employment.** Reducing demand for unauthorized workers is essential to preventing illegal immigration. An employment eligibility verification system is critical in identifying employers whose business model depends on the abuse of workers without legal status. This verification system must be implemented with appropriate regard to privacy and civil rights. Furthermore, only a strong enforcement program that identifies and punishes employers who knowingly employ unauthorized workers as part of their business model will serve as an effective deterrent. Developing a collaborative, interagency approach to bring the combined authorities and enforcement resources of Federal, State, local, tribal, and territorial partners to target abusive employers will reduce demand for unauthorized workers by increasing the penalties against those who exploit them.
- **Eliminate systemic vulnerabilities:** **Prevent fraud, abuse, and exploitation, and eliminate other systemic vulnerabilities that threaten the integrity of the immigration system.** Systemic vulnerabilities that threaten the integrity of the immigration system must be eliminated by identifying and targeting system deficiencies and the root causes of system misuse. Fraud facilitators, criminal and terrorist organizations, and individuals must be prevented from engaging in immigration fraud and violators must be prosecuted. Targeting systemic vulnerabilities may require changing processes, amending regulations, collaborating with other partner agencies, or working with the Congress to strengthen our laws. Information sharing on fraud schemes, trends, immigration crime subjects, and intelligence among Federal, State, local, tribal, and territorial

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

law enforcement partners helps drive decisions and, thus, is a key component of this approach. Timeliness, clarity, and completeness of information are vital to screening operations, immigration decisionmaking, and combating fraud.

- **Prevent entry or admission: Prevent entry or admission of criminals, fugitives, other dangerous foreign nationals, and other unauthorized entrants.** Homeland security efforts must focus on keeping criminal, fugitive, and other dangerous foreign nationals from entering the United States. The use of technology and information sharing among key Federal partners is essential so that dangerous individuals are detected before they are granted an immigration benefit or visa, or are admitted at a port of entry. Threat screening processes, biometric identification, and timely access to information on trends and fraud must all be strengthened to enhance their effectiveness.
- **Arrest, detain, prosecute, and remove: Arrest, detain, prosecute, and remove criminal, fugitive, dangerous, and other unauthorized foreign nationals consistent with due process and civil rights protections.** Dangerous criminal aliens, human rights violators, and other foreign nationals who threaten our national security must be a high priority for law enforcement. This principle also applies when assigning detainees to higher or lower security detention facilities, or when providing alternatives to detention. Arrested individuals must be screened to identify victims of trafficking, refugees, and exploited persons, and they must be provided with access to legal resources.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### MISSION 4: SAFEGUARDING AND SECURING CYBERSPACE

Our security and way of life depend upon a vast array of interdependent and critical networks, systems, services, and resources. To have an infrastructure that is secure and resilient, enables innovation and prosperity, and protects privacy and other civil liberties by design, we must secure cyberspace and manage other risks to its safe use.

#### Key Strategic Outcomes

- Critical information systems and information and communications services are secure, reliable, and readily available.
- Homeland security partners develop, update, and implement guidelines, regulations, and standards that ensure the confidentiality, integrity, and reliability of systems, networks, and data.
- Cyber disruptions or attacks are detected in real-time, consequences are mitigated, and services are restored rapidly.
- Academic institutions produce and homeland security partners sustain a cybersecurity workforce that meets national needs and enables competitiveness.
- Critical infrastructure sectors adopt and sector partners meet accepted standards that measurably reduce the risk of cyber disruption or exploitation.

#### Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment

**Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's information infrastructure.** Cyber infrastructure forms the backbone of the Nation's economy and connects every aspect of our way of life. While the cyber environment offers the potential for rapid technological advancement and economic growth, a range of malicious actors may seek to exploit cyberspace for dangerous or harmful purposes, cause mass disruption of communications or other services, and attack the Nation's infrastructure through cyber means. We must secure the system of networks and information upon which our prosperity relies while promoting economic growth, protecting privacy, and sustaining civil liberties. Both public- and private-sector efforts are required to achieve these aims. In addition, a robust law enforcement and counterintelligence capability is essential to the success of our cybersecurity efforts.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### Objectives

- **Understand and prioritize cyber threats:** Identify and evaluate the most dangerous threats to Federal civilian and private-sector networks and the Nation. The speed of innovation in the cyber realm requires that sharing of information and analysis occur before malicious actors can exploit vulnerabilities. We must continuously sharpen our understanding of risks to our critical information infrastructure. Risk management decisions must incorporate cyber risks based on technological as well as nontechnological factors, and must address the differing levels of security required by different activities. Information and intelligence regarding emerging cyber threats and vulnerabilities must be collected, analyzed, and shared appropriately and promptly. Homeland security partners must provide and receive information and assessments on risks to and incidents involving information systems, networks, and data in time to carry out their risk management responsibilities. Finally, homeland security partners must use compatible information architecture and data standards to maximize the appropriate acquisition, access, retention, production, use, management, and safeguarding of risk information.
- **Manage risks to cyberspace:** Protect and make resilient information systems, networks, and personal and sensitive data. As with other aspects of homeland security, we cannot close every vulnerability and mitigate every risk. Instead, we must develop a risk management approach that accepts certain risks, reduces others, and concentrates on the most consequential. Developing and implementing effective risk management strategies incorporating both protection and resilience for cyber infrastructure will require partnership, coordination, and cooperation across all elements of the homeland security enterprise. Homeland security partners must develop, promulgate, and update guidelines, codes, rules, regulations, and accepted standards when appropriate, that ensure the confidentiality, integrity, and availability of systems, networks, and data without impairing innovation, and while enhancing privacy. Government must focus on and address strategic vulnerabilities in cyberspace. Government must also lead by example, effectively securing its own networks. However, both critical infrastructure sectors and government agencies must meet accepted standards that measurably reduce risk of cyber attack or disruption to public health and safety, critical government services, and essential economic activities. Security controls on information systems, networks, and data must be consistently implemented, monitored, upgraded, and enforced.



## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

- **Prevent cyber crime and other malicious uses of cyberspace:** **Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.** The cyber environment presents the potential for sophisticated cyber threats, cyber espionage, and cyber attacks. We must identify and mitigate cyber threats by coordinating and integrating robust counterintelligence, counterterrorism, intelligence, and law enforcement activities to prevent attacks, disruptions, and exploitations. Through law enforcement efforts, we must identify and locate domestic and international cyber criminals involved in significant cyber intrusions, identity theft, financial crime, and national security-related crimes committed utilizing the Internet. We must ensure that criminal organizations engaged in high-consequence or wide-scale cyber crime are aggressively investigated and disrupted, and their leaders arrested, indicted, and prosecuted. Through counterintelligence efforts, we must identify and thwart hostile intelligence collection activities and other cyber threats directed against the Nation.
- **Develop a robust public-private cyber incident response capability:** **Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.** The evolving nature of cyber threats necessitates that we recognize and respond to cyber incidents in a comprehensive and coordinated fashion involving both the public and private sectors. Cyber disruptions or attacks must be identified in time for a comprehensive response, and homeland security partners must develop and improve cyber incident contingency plans. Additionally, cyber incidents must be managed in accordance with a commonly understood and integrated response framework, and real-time analysis capabilities and processes must mitigate these incidents with an appropriate response. Finally, critical services must be restored and consequences must be mitigated following cyber incidents.

---

### Goal 4.2: Promote Cybersecurity Knowledge and Innovation

---

**Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.** Cybersecurity is a dynamic field, and cyber threats and challenges evolve at breathtaking speed. Education, training, awareness, science, technology, and innovation must flourish in order to meet this challenge. While we must protect the Nation from cyber attacks that occur today, we must also prepare now to mitigate the most consequential cybersecurity risks that the United States and its people will face in 5, 10, and 20 years. We must make long-term investments that sustain a safe, secure, and reliable cyber environment, enable prosperity, further

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

social and community uses of the Internet, and facilitate transactions and trade, while safeguarding privacy and civil liberties.

### Objectives

- **Enhance public awareness: Ensure that the public recognizes cybersecurity challenges and is empowered to address them.** As we have seen in other homeland security mission areas, an aware and empowered public is our best defense against threats, and our greatest resource in building resilience and fostering innovation. Each individual, every business enterprise, and each government agency has a vital role to perform if cyberspace is to realize its full potential. For the Nation to remain secure and prosperous, government must not only succeed at its own cybersecurity mission but must also empower others to succeed in theirs. Communications to the public must emphasize their role in cybersecurity. Leaders in the public and private sectors must be more informed of the security implications of their decisions with respect to cyberspace.
- **Foster a dynamic workforce: Develop the national knowledge base and human capital capabilities to enable success against current and future threats.** A capable workforce must exist to protect cyber infrastructure from current, emerging, and future risks. A knowledgeable cybersecurity workforce must exist across government with sufficient capacity and expertise to manage current and emerging risks. We must better understand our own cyber strengths and weaknesses and those of our adversaries. Through learning, we can adapt and recalibrate our approaches, our areas of emphasis, and our operational objectives.
- **Invest in innovative technologies, techniques, and procedures: Create and enhance science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.** Cyberspace's inherent characteristics demand constant innovation in order to effectively counter threats. Small vulnerabilities can lead to severe challenges in securing the Nation's vast – and vastly critical—information infrastructure. Relatively small investments in adversary attack capabilities can require disproportionately large investments in defense. Technology will assist us, and better ways of using technology and people will allow us to bring capabilities to bear more effectively. There must be continuous emphasis on cyber research, development, innovation, and interoperability, which drives advances in technologies, techniques, and procedures. As part of the homeland security enterprise, government should work creatively and collaboratively with the private sector to identify tailored solutions that both take into account the need

## **V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY**

to protect public and private interests and take an integrated approach to achieving clear objectives, preventing mass disruptions and exploitations of government systems and critical infrastructure through cyberspace. We must prioritize investment in programs that demonstrate the best opportunity to help mitigate national cyber risk. Innovation in technology, practice, and policy must further protect --not erode-- privacy and civil liberties.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### MISSION 5: ENSURING RESILIENCE TO DISASTERS

The strategic aims and objectives for ensuring resilience to disasters are grounded in the four traditional elements of emergency management: hazard mitigation, enhanced preparedness, effective emergency response, and rapid recovery. Together, these elements will help create a Nation that understands the hazards and risks we face, is prepared for disasters, and can withstand and rapidly and effectively recover from the disruptions they cause.

#### Key Strategic Outcomes

- A standard for general community hazard mitigation is collaboratively developed and adopted by all communities.
- Individuals and families understand their responsibilities in the event of a community-disrupting event and have a plan to fulfill these responsibilities.
- Preparedness standards for life safety, law enforcement, mass evacuation and shelter-in-place, public health, mass care, and public works capabilities, including capacity levels for catastrophic incidents, have been developed and are used by all jurisdictions.
- Jurisdictions have agreements in place to participate in local, regional, and interstate mutual aid.
- All organizations with incident management responsibilities utilize the *National Incident Management System*, including the Incident Command System, on a routine basis and for all federally declared disasters and emergencies.

#### Goal 5.1: Mitigate Hazards

##### Strengthen capacity at all levels of society to withstand threats and hazards.

Though the occurrence of some disasters is inevitable, it is possible to take steps to reduce the impact of damaging events that may occur. The Nation's ability to withstand threats and hazards requires an understanding of risks and robust efforts to reduce vulnerabilities. Mitigation provides a critical foundation to reduce loss of life and property by closing vulnerabilities and avoiding or lessening the impact of a disaster, thereby creating safer communities. Mitigation seeks to break out of the cycle of disaster damage, reconstruction, and repeated damage. Mitigating vulnerabilities reduces both the direct consequences and the response and recovery requirements of disasters.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### Objectives

- **Reduce the vulnerability of individuals and families: Improve individual and family capacity to reduce vulnerabilities and withstand disasters.** Individuals and families must be a focal point of mitigation efforts, as they are best positioned to reduce their own vulnerabilities. Promoting individual and family mitigation requires identifying the factors that influence the psychological and social resilience of individuals. Government must actively engage to help individuals understand the risks that their communities face, the resources available to them, and the steps they can take to prepare themselves, their homes, and their businesses.
- **Mitigate risks to communities: Improve community capacity to withstand disasters by mitigating known and anticipated hazards.** Community-level mitigation measures have historically proven successful in reducing the effects of disasters. Standards for general community hazard mitigation, such as building codes and land and water use policies, must be in place and enforced around the country. In addition, measures to reduce the consequences of disasters on critical infrastructure and essential systems and services, including supply chains, health care systems, communications networks, and transportation systems, must be incorporated into development planning. Insurance policies—including those offered or otherwise supported by the Federal Government—should include hazard mitigation incentives.

---

### Goal 5.2: Enhance Preparedness

---

**Engage all levels and segments of society in improving preparedness.** Active participation by all segments of society in planning, training, organizing, and heightening awareness is an essential component of national preparedness. While efforts have traditionally focused on the preparedness of government and official first responders, individuals prepared to care for themselves and assist their neighbors in emergencies are important partners in community preparedness efforts. Because neighbor-to-neighbor assistance, when done safely, decreases the burden on first responders, individuals should be seen as force multipliers who may also offer specialized knowledge and skills.

### Objectives

- **Improve individual, family, and community preparedness: Ensure individual, family, and community planning, readiness, and capacity-building for disasters.** Prepared individuals and families enhance overall

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

community resilience and reduce the burden on government emergency responders. Individuals and families must be prepared to care for themselves for a reasonable period of time after a disaster—some experts have suggested the first 72 hours—and assist their neighbors, reserving scarce public resources to assist those who are injured, incapacitated, or otherwise unable to care for themselves. The public must be engaged in order to build a collective understanding of their risks, the resources available to assist their preparations, and their roles and responsibilities in the event of a disaster. Participation in community disaster response programs such as Community Emergency Response Teams (CERTs), other Citizen Corps programs, and similar volunteer teams maintained by nongovernmental organizations must be enhanced, and community-based training and exercises must be increased, to help individuals gain the skills necessary to respond to disasters safely and in coordination with local authorities. Community organizations, including local NGOs, faith-based groups, and advocacy groups for vulnerable populations—often cornerstones of communities, but not traditionally involved in emergency management—must be integrated into community planning, risk reduction, and preparedness activities.

- **Strengthen capabilities: Enhance and sustain nationwide disaster preparedness capabilities, to include life safety, law enforcement, mass evacuation and shelter-in-place, public health, mass care, and public works.** Homeland security partners must be prepared for the variety of requirements resulting from a disaster. Joint hazard identification and risk analysis can help determine consensus-based, tiered preparedness standards for States, regions, and localities. These preparedness standards will then allow us to develop nationally the capabilities we will need to address the full range of threats and hazards that we face.

Because success in day-to-day operations often foreshadows success in larger incidents, critical emergency response capabilities must be enhanced and all organizations with incident management responsibilities must be encouraged to use the Incident Command System (ICS) or a comparable system compliant with the *National Incident Management System* for day-to-day emergencies. In addition, we must evaluate our performance in exercises and learn from our responses to actual incidents to identify and close capability and capacity gaps and improve response and recovery operations.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

### Goal 5.3: Ensure Effective Emergency Response

**Strengthen response capacity nationwide.** Because it is impossible to eliminate all risks, a resilient Nation must have a robust capacity to respond when disaster strikes. Such response must be effective and efficient and grounded in the basic elements of incident management. When an incident occurs that is beyond local response capabilities, communities must be able to obtain assistance from neighboring jurisdictions and regional partners quickly, making a robust regional capacity vital to effective emergency response.

#### Objectives

- Provide timely and accurate information to the public;  
Establish and strengthen pathways for clear, reliable, and current emergency information, including effective use of new media.

Timely, appropriate, and reliable communication with the public before, during, and immediately after disasters is a key component of societal resilience. In today's environment of speed-of-light communications and pervasive social networking technologies, homeland security partners must take full advantage of cutting-edge tools and capabilities to promote widespread situational awareness. As such, information sharing and public alert and warning must be viewed as mutually supportive efforts in seeking to combine the networked power of new media and "Web 2.0" technologies with existing homeland security information-sharing capabilities such as fusion centers, emergency operations centers, and joint terrorism task forces. Moreover, emergency information must be accessible through as many pathways as

**Less than three minutes after American Airlines Flight 77 crashed into the Pentagon,** Arlington County Fire Department officials were on scene, leading the effort to establish a unified command and control structure under protocols set forth in the Incident Command System (now part of the *National Incident Management System*) and the Federal Response Plan (a predecessor to today's *National Response Framework*). These interagency emergency management frameworks were well known to first responders because of common regional use, extensive training, and operational experience in the field. In the hours following the attack, thousands of personnel from some 50 public safety agencies at the Federal, State, and local levels arrived on site and at nearby staging areas and emergency operations centers. Their decades of joint planning, training, exercising, and operations had built the foundations of a regional homeland security community, which ensured a universal understanding of roles and responsibilities and allowed for a near-seamless integration of multiple agencies into a unified and effective response.

## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

possible, to include multiple languages, through social networks in low-income areas, and to those with special needs.

- **Conduct effective disaster response operations:** **Respond to disasters in an effective and unified manner.** An effective response requires that incident management organizations at all levels of government embrace common doctrine, undertake joint planning and training, and work to establish interoperable communications and equipment capabilities across jurisdictions, providing the flexibility, adaptability, and scalability necessary to match the complexity of many modern disasters. This cohesion will allow responders to improvise effectively in the face of unforeseen circumstances. First responders must be able to use the on-scene command, resource management, and communications and information management elements of the *National Incident Management System*. Jurisdictions across the Nation must have the ability to accurately characterize incidents and track the status of personnel and resources responding to major disasters and emergencies.
- **Provide timely and appropriate disaster assistance:** **Improve governmental, nongovernmental, and private-sector delivery of disaster assistance.** Effectively delivering disaster assistance requires improved coordination and preparedness among governmental, nongovernmental, and private-sector resources, including local businesses and faith-based and community organizations. Humanitarian relief services such as emergency sheltering and individual financial assistance must be efficiently and effectively administered. Effective operations during disasters require integration of nongovernmental assets in planning, training, and exercises.

---

### Goal 5.4: Rapidly Recover

---

**Improve the Nation's ability to adapt and rapidly recover.** Major disasters and catastrophic events produce changes in habitability, the environment, the economy, and even in geography that can often preclude a return to the way things were. We must anticipate such changes and develop appropriate tools, knowledge, and skills to adapt, improve sustainability, and maintain our way of life in the aftermath of disaster. Recent events have highlighted the challenges we face in dealing with disaster recovery. From sheltering and rehousing displaced survivors to reconstituting critical infrastructure and reestablishing the economic base of devastated areas, the challenges are profound. Individuals, businesses, nonprofit organizations, local, tribal, State, and Federal governments all have responsibilities



## V. MISSIONS, GOALS, AND OBJECTIVES OF HOMELAND SECURITY

in disaster recovery, underscoring the need to improve coordination and unity of effort.

### Objectives

- **Enhance recovery capabilities:** Establish and maintain nationwide capabilities for recovery from major disasters. Nationwide—at all levels of government and in nongovernmental organizations—sufficient capabilities for disaster recovery must be developed and maintained. While no government program can make communities and individuals whole, we must do a better job with the limited resources we have. This requires the development of a national strategic approach for disaster recovery and the use of standards for enhanced recovery capabilities. Federal roles and responsibilities must be clarified, and all jurisdictions must maintain and exercise recovery plans.
- **Ensure continuity of essential services and functions:** Improve capabilities of families, communities, private-sector organizations, and all levels of government to sustain essential services and functions. Communities, government entities, and private-sector organizations must develop and exercise continuity plans. Business continuity standards and practices must continue to gain acceptance. During a disaster, families and communities, as well as businesses and governmental entities, must be able to sustain critical capabilities and restore essential services in a timely manner.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE



The strategic aims and objectives for maturing and strengthening the homeland security enterprise are drawn from the common themes that emerge from each of the mission areas. Ensuring a shared awareness and understanding of risks and threats, building capable communities, creating unity of effort, and enhancing the use of science and technology underpin our national efforts to prevent terrorism and enhance security, secure and manage our borders, enforce and administer our immigration laws, safeguard and secure cyberspace, and ensure resilience to disasters.

---

### Enhance Shared Awareness of Risks and Threats

---

**Establish a comprehensive system for building and sharing awareness of risks and threats.** The engine behind a distributed homeland security effort is a shared awareness of the risks and threats among all key stakeholders. To be effective, the homeland security enterprise requires a comprehensive information strategy that respects the privacy and civil liberties of individuals, as well as the diversity of information needs across the different missions. Although much has been done to improve information sharing since the 9/11 attacks, more work remains. Toward that end, the following key objectives are a priority: national-level homeland security risk assessments; tools and institutional arrangements for effective and timely sharing of information and analysis; a robust approach to screening and identification verification that safeguards individual privacy and civil rights; enhanced knowledge management tools; improved domain awareness, including the expanded use of sensors, detectors, and other unmanned systems across a wide range of homeland security activities; and aggressive activities to identify and defeat efforts by adversaries to conduct surveillance against homeland targets and exploit any weaknesses. These objectives must culminate in a common understanding of security as a shared responsibility.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

### Objectives

- Establish an approach to national-level homeland security risk assessments:**  
Develop and implement a methodology to conduct national-level homeland security risk assessments. Constructing a nationwide approach to homeland security requires a deliberate analytic method to evaluate the risks posed by various hazards and threats to national strategic interests and establish strategic guidance for homeland security prioritization. Given limited resources and the prospect of a seemingly infinite possibility of threats and vulnerabilities to consider, we must make difficult decisions about how to prioritize homeland security efforts. A national homeland security risk assessment will provide the Nation's homeland security leaders with an assessment of risks to our strategic interests from the full range of threats, hazards, challenges, and long-term trends. Understanding the risks and the ability of DHS and partners and stakeholders across the homeland security enterprise to reduce and manage these risks is a fundamental step toward informing our priorities and the allocation of resources. The Federal Government should develop a methodology for a homeland security national-level risk assessment. This national-level risk assessment should include threat assessments produced by the Intelligence Community, as well as the information and expertise concerning vulnerabilities and consequences resident across Federal departments and agencies and the homeland security enterprise. National-level homeland security risk assessments will enable DHS and homeland security partners and stakeholders to take the next step toward truly risk-informed decisionmaking.

### A Homeland Security National Risk

**Assessment** will provide the Nation's homeland security leaders with an assessment of homeland security risks to our national strategic interests from challenges that include weapons of mass destruction, global terrorism, mass cyber attacks, pandemics, major accidents and natural disasters, illegal trafficking and related transnational criminal activity, and smaller scale attacks. Such a risk assessment will help homeland security decisionmakers determine the most promising strategic opportunities to manage risks across the homeland security enterprise.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

- Share information and analysis:** Enhance critical tools and institutionalize arrangements for timely access and effective sharing of information and analysis. The ability to more effectively share information among local, tribal, territorial, State, and Federal homeland security practitioners is critical to improving collaboration and decisionmaking during day-to-day operations and large-scale emergencies. Integrating existing technologies and using tools such as State and major urban area fusion centers provide critical delivery vehicles for homeland security intelligence and information. We must continue to strengthen baseline capabilities and analytic capacity to operate consistently, rapidly identify and disseminate information, and support and enhance a State and urban area intelligence platform for risk-based, information-driven decisionmaking by homeland security stakeholders.
- Screen and verify identity:** Establish a robust approach to identity verification that safeguards individual privacy and civil rights. Robust procedures to screen and verify identities are critical to helping accurately identify people and assess risk. Future systems will need to be increasingly secure, efficient, easy to use, and flexible. Ongoing research into emerging technologies will help to expand screening and verification capabilities. At the same time, we must adhere to privacy standards and ensure that we fully respect individual rights and liberties. Information needed to achieve homeland security objectives must be collected and used consistent with applicable law and policy. Training, audits, and other oversight mechanisms are essential to ensuring information is used lawfully and appropriately.

**Effective, timely sharing of information and analysis** is essential to homeland security. Fusion centers are the State and major city entities that were recommended in the Implementing the 9/11 Commission Recommendations Act of 2007 as the best way for Federal, State, local, tribal, and territorial governments and the owners and operators of critical infrastructure to share information and intelligence about terrorist threats, criminal activity, and other hazards. Since 2006, States and major cities have stood up some 70 fusion centers across the country, with the Federal Government contributing personnel, financial, and technical support.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

- Enhance domain awareness:** Ensure shared situational awareness in the air, land, and maritime domains. Homeland security activities depend upon having shared situational awareness across a range of complex and dynamic operational environments. Awareness of aircraft, vehicles, and vessels in U.S. airspace and the air, land, and maritime approaches to the United States, along with Federal, State, local, tribal, territorial, and international resources to address threats and hazards, is critical to our ability to take effective action. Sensors, detectors, and other unmanned systems can play a vital role in supporting decisions about whether threats are present and when to intervene. Numerous unmanned systems are in use or development across the homeland security enterprise, including systems for monitoring the integrity of shipping containers from the point of consolidation to the point of deconsolidation; a “lab-in-a-box” capable of aerosol collection, molecular identification, and reporting on biological threats; imaging and radar systems designed to detect, track, and classify contacts; sensors to monitor the vital signs and establish the physical health of first responders; and a first responder locating system to enable incident commanders to visually track personnel. We must increase our domain awareness efforts consistent with our core interests of privacy and civil liberties.
- Integrate counterintelligence:** Use and integrate counterintelligence in all aspects of homeland security to thwart attacks against the homeland. The foreign intelligence threat to the United States—from states, non-state actors, and terrorist groups—is pervasive, intricate, far reaching, and growing. Globalization has made communication technology widely available, which our enemies can manipulate to gain advantages in the international marketplace and against the homeland, including our critical infrastructure. Because terrorists or

### Hybrid Capabilities and Complementary

**Activities.** Hybrid capabilities—assets and resources capable of performing multiple missions—are a hallmark of homeland security. In some cases, the same assets and personnel that patrol our borders, enforce our immigration laws, and respond to major oil spills, for example, also enforce safety regulations, assist travelers, and safeguard natural resources. These complementary activities are critical to fulfilling other national interests, and are often intertwined and mutually supporting with homeland security activities. Homeland security partners and stakeholders—both within DHS and across the homeland security enterprise—often maintain hybrid capabilities to fulfill multiple missions.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

other adversaries often employ intelligence tradecraft to identify targets and prepare their attacks, counterintelligence can provide a critical means to understanding current and evolving threats. Counterintelligence also provides a suite of tools and skills to identify, deceive, exploit, or disrupt these preparations and operations. Efforts to prevent terrorism and enhance the security of the homeland rely, in part, on effective counterintelligence. We must disrupt hostile cyber activities, identify hostile intelligence collection activities, detect insider threats, and expand awareness of our adversaries' intelligence threats and capabilities.

- **Establish a common security mindset: Promote a common understanding of security as a shared responsibility.** Homeland security is a shared responsibility for which all elements of society—from individuals and communities, to the private sector, to State, local, tribal, and territorial governments, to nongovernmental organizations, to the Federal Government—have a vital role to play. The Federal Government cannot be everywhere, nor can it alone ensure resilience or thwart every threat, despite best efforts. Private individuals, communities, and other nongovernmental actors must be empowered to take action. The American people hold a strong sense of community, a belief in collective responsibility, and a willingness to do what is required of them to contribute to our common security and sustain our way of life. The highest calling of the homeland security enterprise is to empower Americans to contribute to our country's security—to embrace a unity of purpose. Empowered individuals with a mindset of shared responsibility are uniquely capable of disrupting threats and ensuring the security of the interdependent systems that make up society. Individuals and communities are the focal point of societal resilience, enhancing public preparedness and thus diminishing the effectiveness of terrorist tactics.

---

### Build Capable Communities

---

**Foster communities that have information, capabilities, and resources to prevent threats, respond to disruptions, and ensure their own well-being.** Individuals, families, and communities are essential partners in the homeland security enterprise. Building and sustaining capability at the community level is essential to meeting homeland security strategic aims and realizing our vision for a secure homeland.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

### Objectives

- **Set capability and capacity standards:** Identify core capability and capacity targets to guide homeland security investments and activities across the enterprise. We must focus on building and maintaining capabilities to address challenges across all homeland security missions. To do this, we must jointly, through cross-governmental collaborative mechanisms, set clear, measurable target levels of capability and capacity for enterprise partners across all missions and develop a system for assessing progress toward these targets. In order to succeed, we must focus our efforts on concrete, specific, and measurable objectives, setting clear, measurable target levels of capability and capacity for enterprise partners. Commitment to such a process is essential to our ability to “spend smarter” in an environment of tightening resources.
- **Enhance systems for training, exercising, and evaluating capabilities:** Training provides first responders, homeland security officials, emergency management officials, nongovernmental and private-sector partners, and other personnel with the knowledge, skills, and abilities needed to perform key tasks required by specific capabilities. Exercises provide a vital tool for homeland security personnel, from first responders to senior officials, to practice operational activities and decisionmaking processes in a realistic but risk-free environment. We must build on current efforts to coordinate and integrate exercises nationally, and emphasize the importance of exercising both steady-state and contingency-based mission activities in order to achieve measurable improvement. Exercises must also be valuable tools for assessing and improving performance, while demonstrating community resolve to prepare for major incidents. We must strive for assessments of

### State, local, tribal, and territorial governments

are on the front lines of our efforts to secure our homeland, and are the first responders to incidents of all types. A coordinated approach that promotes unity of effort will provide the strongest foundation for the homeland security enterprise’s efforts to combat current, emerging, and future threats to the homeland. To achieve unity of effort, partners will need clearly defined roles and responsibilities, access to information, and a shared understanding of how risks are managed and prioritized to inform the allocation of limited resources. In addition, Federal, State, local, tribal, and territorial partners will need a common framework to understand threats, assess risks, and share information.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

capabilities across all levels that minimize the volume of reporting requirements and more efficiently collect necessary data on homeland security capabilities.

- **Maintain and sustain equipment and capabilities:** **Promote smart investment in operational capabilities.** Homeland security equipment and capabilities are critically important yet resource-intensive investments for stakeholders across the enterprise. In a resource-constrained environment, it is critical that the maintenance and sustainment of capabilities is done in the most cost-effective manner possible. We must promote and support long-term investments in capabilities through our grant programs and other funding mechanisms. Our goal is to help create capable communities, and we should promote the most efficient and prudent means of achieving and sustaining that goal.

---

### Foster Unity of Effort

---

**Foster a broad national culture of cooperation and mutual aid.** Unity of effort is the ultimate goal for maturing and strengthening the homeland security enterprise. Cooperation and mutual aid are cornerstones of success for effective joint activity. A coordinated approach that promotes unity of effort will provide the strongest foundation to combat current, emerging, and future threats to the homeland. To achieve unity of effort, partners will need clearly defined roles and responsibilities, access to information, and a shared understanding of how risks are managed and prioritized to inform the allocation of limited resources. In addition, public-sector agencies and their private-sector partners will need an integrated framework to share information, understand threats, and assess and manage risks.

#### Objectives

- **Build a homeland security professional discipline:** **Develop the homeland security community of interest at all levels of government as part of a cadre of national security professionals.** A well-documented need within the national security community is a professional development program that fosters a stable and diverse community of professionals with the proper balance of relevant skills, attributes, experiences, and comprehensive knowledge. Executive Order 13434, "National Security Professional Development," initiated a program for developing interagency national security professionals through access to an integrated framework of training, education, and professional experience opportunities. We must work together with our national security partners in bringing that important idea to fruition. As part of that effort, we must take steps to create a homeland security community of interest across the



## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

enterprise. Three elements of professional development are education, training, and experience via developmental assignments. State, local, tribal, and territorial governments, DHS and other Federal agencies, and academic institutions have taken important steps to build programs to support these key areas and will continue to emphasize enterprise-wide approaches to enhancing homeland security professional development.

- **Promote regional response capacity:** **Promote mutual aid agreements for response requirements that exceed local capacity.** As previously mentioned, disasters rarely recognize jurisdictional boundaries and often overwhelm local response capabilities. For these situations, regional plans should be developed to address operational interdependencies and local, regional, and interstate mutual aid agreements must be in place. To ensure interoperability, incident management organizations at all levels of government should employ elements of the *National Incident Management System* and conduct regional joint assessments, planning, and training. This objective builds on the foundation established in Mission 5: Ensuring Resilience to Disasters.
- **Institutionalize homeland security planning:** **Develop a planning system to execute homeland security activities.** A homeland security planning system is essential and indispensable to homeland security. Current planning systems address only portions of overall homeland security activities, and require better integration across all levels of government and with nongovernmental entities. Through fully considered interagency and intergovernmental discussions, we must integrate current planning practices and, drawing from best practices across the homeland security enterprise, create a planning system that allows homeland security partners and stakeholders to plan collaboratively and ensure that homeland security activities achieve our shared goals.
- **Further enhance the military-homeland security relationship:** **Strengthen unity of effort between military and civilian activities for homeland**

**Unity of effort** is the key to operational success in homeland security. Jointness and multiagency coordination principles underpin both military and civilian mechanisms for achieving unity of effort. The *National Response Framework* and *National Incident Management System* facilitate unity of effort for disaster response and emergency services activity. The *Maritime Operational Threat Response Plan* and the Joint Interagency Task Force concept are used to achieve unity of effort for preventing terrorism, securing cyberspace, and effectively controlling U.S. land, air, and sea borders.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

**security.** We must work together to develop and expand models of coordination and cooperation between military and civilian authorities, and revise strategy and doctrine accordingly. The *National Response Framework* and the *National Incident Management System* provide mechanisms to ensure unity of effort between civilian and military authorities for disaster response. We must continually refine and enhance the framework for providing defense support to civil authorities for all homeland security mission activities. In addition, Federal departments and agencies should jointly conduct planning and analysis for homeland security and related defense activities, including developing joint strategic planning and analytic tools for determining capability requirements, as well as conducting joint national-level risk assessments in areas of shared interest. Federal departments and agencies must also explore ways to jointly develop capabilities necessary for both defense and homeland security.

- **Strengthen the ability of Federal departments and agencies to support homeland security missions.** While some Federal departments and agencies have broad homeland security responsibilities, others have smaller, but still critical, homeland security roles or capabilities associated within their own statutorily authorized programs, which may be leveraged for homeland security purposes. Federal departments and agencies with smaller, but critical, homeland security roles must be adequately resourced to meet homeland security mission requirements.
- **Expand and extend governmental and private-sector international partnerships: Transform how government and the private sector interact.** International partners are key participants in the homeland security enterprise. The interconnected nature of world economies and international infrastructure means that seemingly isolated events often have transnational origins and global consequences. The acceleration of the flows of ideas, goods, and people around the world and across U.S. borders generally advances America's interests, but also creates security challenges that are increasingly borderless and unconventional. International partners are critical to the effort to secure the homeland against threats that transcend jurisdictional and geographic boundaries. International engagement enhances the transparency of threat trajectories and increases our capacity to understand, investigate, and interdict threats at the earliest possible point, ideally before they become manifest, reach our shores, or disrupt the critical networks on which we depend. The United States must work with its international partners to increase global security.

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

against terrorism and violent extremism, the spread of infectious diseases, and the consequences of natural disasters.

- **Mature the Department of Homeland Security: Improve DHS's organizational and programmatic alignment and its management systems and processes.** DHS must lead by example. Ensuring unity of effort across the homeland security enterprise requires unity of effort within the Department. Critical to unifying DHS is improved organizational alignment, particularly among DHS headquarters components, enhanced programmatic alignment to the homeland security missions, and more efficient and effective management processes, including strategic planning, performance management, and accounting structure. DHS must complete a thorough review of its own organizational structures and programmatic activities, align programs and budgets to homeland security missions, and strengthen its management processes. This work began during the QHSR process and continues through the Department's bottom-up review.

---

### **Foster Innovative Approaches and Solutions Through Leading-Edge Science and Technology**

---

**Ensure scientifically informed analysis and decisions are coupled to innovative and effective technological solutions.** We must be able to address a highly dynamic, broad, and ever-changing spectrum of threats, vulnerabilities, and disaster scenarios and to design and implement cost-effective operational and technological solutions across a wide array of operational contexts, in a manner that protects American values. Although many of the security threats now confronting the United States are driven by the global diffusion of technology, science and technology can also provide new and more effective methods for preventing and mitigating these threats, as well as natural disasters. The Federal Government must have a robust research effort in homeland security that is grounded in sound science, and a rigorous and disciplined approach to technology development, acquisition, and deployment.

#### **Objectives**

- **Scientifically study threats and vulnerabilities: Pursue a rigorous scientific understanding of current and future threats to homeland security and the possible means to their prevention and mitigation.** A comprehensive and vivid understanding of the probability and potential consequences of homeland security threats and hazards and the relative risk they pose forms the strategic foundation of the homeland security enterprise. Ongoing analyses of threats,

## VI. MATURING AND STRENGTHENING THE HOMELAND SECURITY ENTERPRISE

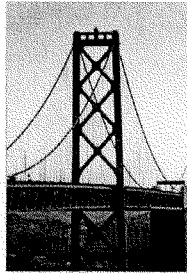
vulnerabilities, and the efficacy of our countermeasures by both the public and private sectors will inform homeland security priorities and help ensure that investments and operations focus on the most urgent problems and the most effective means for addressing them.

- **Develop innovative approaches and effective solutions:** Encourage and enable innovative approaches to critical homeland security challenges, fostering collaborative efforts involving government, academia, and the private sector. Achieving the goals of the core homeland security missions will require scientific research to discover new knowledge and methods that can be applied to homeland security challenges, and the creation of new technologies and new ways of thinking about problems and possible solutions. Technological feasibility, operational requirements, training needs, and financial sustainability must all be considered in developing and deploying new technologies. We must seek to foster a rich and wide-ranging capacity to identify and think through complex and unfamiliar problems and to formulate effective and inventive solutions spanning many difficult and varied operational contexts. We must engage a wide range of stakeholders in this endeavor, including government labs, universities, federally funded research and development centers, and the private sector.

**DHS and the Department of Energy—including the National Laboratories—have established a partnership on aviation security** in order to develop new and more effective technologies to deter and disrupt known threats and proactively anticipate and protect against new ways by which terrorists could seek to board an aircraft.

This page intentionally left blank.

## VII. CONCLUSION: THE PATH FORWARD



The Quadrennial Homeland Security Review report sets forth a broad vision for homeland security. We have learned that our Nation's security is more than building protections, securing our borders, or preventing terrorism, although these measures are all central to homeland security. Homeland security is also about protecting the American way of life and ensuring our resilience in a challenging world.

The QHSR process (elaborated at **Appendix B**) and resulting report were designed to serve as a catalyst to spur the continued evolution and maturation of our Nation's homeland security enterprise—the diverse and distributed set of public and private actors from all corners of this Nation. Through this effort, we seek to foster a greater understanding of our shared responsibility and growing capability to protect ourselves from a range of threats and hazards.

In the years ahead, the world will be filled with breathtaking technological changes, social advances, and an accelerating flow of ideas, goods, and people around the world. These advancements and global interactions will enrich and improve our lives, but they may also be exploited by or may contribute to violent extremism, terrorist attacks, health threats, proliferation concerns, natural disasters, and cyber attacks—with many of these occurring, perhaps, at the same time.

The QHSR has set the stage for detailed analyses of homeland security capabilities and requirements across the homeland security enterprise. Stakeholders must now work to prioritize and identify the capabilities needed to achieve the goals, objectives, and outcomes identified in the QHSR, tie these requirements to resource allocation priorities, set performance criteria, and validate the allocation of roles and responsibilities.

The division of operational roles and responsibilities among Federal departments and agencies for various homeland security mission goals and objectives emerged as a major area requiring further study following the QHSR. Going forward, an analysis of roles and responsibilities across the homeland security missions would help resolve gaps or unnecessary redundancies between departments and agencies. Meaningful engagement by representative stakeholders from across the homeland security enterprise, including State, local, tribal, and territorial governments, must be part of the process.

## VII. CONCLUSION: THE PATH FORWARD

The Department of Homeland Security has begun a comprehensive examination of the Department's activities and resources. This bottom-up review is a major step forward in DHS's ongoing effort to systematically link strategy to program to budget. The objective of this sequence of reviews is a linked strategy, set of programs, and budget that will strengthen the Department. The QHSR, the bottom-up review, and the budget proposals that will follow are important steps in maturing DHS into a truly strategy-driven organization. Additionally, the bottom-up review will advance the Department's functionality in three ways:

1. Increased comparability of programs, activities, and resources within and across components;
2. Improved measurement of desired mission outcomes and the contribution of programs, activities, and resources to these mission outcomes; and
3. Better cost estimating of programs and activities.

This exercise entails mapping existing activities to QHSR missions, identifying gaps and overlaps in these activities, improving the Department's ability to analytically relate activities to mission outcomes, and reassessing how to organize and group these activities into programs.

The path forward following the QHSR is clear—we must move with a sense of urgency and purpose to achieve our shared interest and common vision of a safer, more secure and resilient America. Each of us—government, business enterprise, and individual alike—has a role to play, contributing to the collective strength of this country. The message is clear: This Nation can protect itself. But we must all play a role—and in the commitment of each, we will secure the homeland for all.

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

Homeland security spans the authorities and responsibilities of Federal departments and agencies, State, local, tribal and territorial governments, the private sector, as well as private citizens and communities. For this reason, coordination and cooperation are essential to successfully carrying out and accomplishing the homeland security missions. Documents such as the *National Infrastructure Protection Plan* (NIPP) and *National Response Framework* (NRF), as well as documents produced by the National Counterterrorism Center, spell out roles and responsibilities for various aspects of homeland security. The following discussion highlights key current roles and responsibilities of the many actors across the homeland security enterprise. They are derived largely from statutes, Presidential directives, and other authorities, as well as from the NIPP and NRF.

- The **President of the United States** is the Commander in Chief and the leader of the Executive Branch of the Federal Government. The President, through the National Security and Homeland Security Councils and the National Security Staff, provides overall homeland security policy direction and coordination. As a result of Presidential Study Directive 1 (2009), which directed an examination of ways to reform the White House organization for counterterrorism and homeland security, the White House merged the staffs of the National Security Council and the Homeland Security Council into a single new integrated National Security Staff.
- The **Secretary of Homeland Security** leads the Federal agency as defined by statute charged with homeland security: preventing terrorism and managing risks to critical infrastructure; securing and managing the border; enforcing and administering immigration laws; safeguarding and securing cyberspace; and ensuring resilience to disasters.
- The **Attorney General** has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, as well as for related intelligence collection activities within the United States. Following a terrorist threat or an actual incident that falls within the criminal jurisdiction of the United States, the Attorney General identifies the perpetrators and brings them to justice. The Attorney General leads the Department of Justice, which also includes the **Federal Bureau of Investigation**, **Drug Enforcement Administration**, and **Bureau of Alcohol, Tobacco, Firearms, and Explosives**, each of which has key homeland security responsibilities.
- The **Secretary of State** has the responsibility to coordinate activities with foreign governments and international organizations related to the prevention.



## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

preparation, response, and recovery from a domestic incident, and for the protection of U.S. citizens and U.S. interests overseas. The Department of State also adjudicates and screens visa applications abroad.

- The **Secretary of Defense** leads the Department of Defense (DOD), whose military services, defense agencies, and geographic and functional commands defend the United States from direct attack, deter potential adversaries, foster regional stability, secure and assure access to sea, air, space, and cyberspace, and build the security capacity of key partners. DOD also provides a wide range of support to civil authorities at the direction of the Secretary of Defense or the President when the capabilities of State and local authorities to respond effectively to an event are overwhelmed.
- The **Secretary of Health and Human Services** leads the coordination of all functions relevant to Public Health Emergency Preparedness and Disaster Medical Response. Additionally, the Department of Health and Human Services (HHS) incorporates steady-state and incident-specific activities as described in the National Health Security Strategy. HHS is the coordinator and primary agency for Emergency Support Function (ESF) #8 – Public Health and Medical Services, providing the mechanism for coordinated Federal assistance to supplement State, local, tribal, and territorial resources in response to a public health and medical disaster, potential or actual incident requiring a coordinated Federal response, and/or during a developing potential health and medical emergency. HHS is also the Sector-Specific Agency for the Healthcare and Public Health Sector.
- The **Secretary of the Treasury** works to safeguard the U.S. financial system, combat financial crimes, and cut off financial support to terrorists, WMD proliferators, drug traffickers, and other national security threats.
- The **Secretary of Agriculture** provides leadership on food, agriculture, natural resources, rural development, and related issues based on sound public policy, the best available science, and efficient management. The Department of Agriculture (USDA) is the Sector-Specific Agency for the Food and Agriculture Sector, a responsibility shared with the Food and Drug Administration with respect to food safety and defense. In addition, USDA is the coordinator and primary agency for two Emergency Support Functions: ESF #4 – Firefighting and ESF #11 – Agriculture and Natural Resources. USDA, together with the Department of the Interior, also operates the National Interagency Fire Center.

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

- The **Director of National Intelligence** serves as the head of the Intelligence Community (IC), acts as the principal advisor to the President and National Security Council for intelligence matters relating to national security, and oversees and directs implementation of the National Intelligence Program. The IC, composed of 16 elements across the U.S. Government, functions consistent with law, Executive order, regulations, and policy to support the national security-related missions of the U.S. Government. It provides a range of analytic products that assess threats to the homeland and inform planning, capability development, and operational activities of homeland security enterprise partners and stakeholders. In addition to IC elements with specific homeland security missions, the Office of the Director of National Intelligence maintains a number of mission and support centers that provide unique capabilities for homeland security partners, including the **National Counterterrorism Center (NCTC)**, National Counterproliferation Center, and National Counterintelligence Executive. NCTC serves as the primary U.S. government organization for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, and conducts strategic operational planning for integrated counterterrorism activities.
- The **Secretary of Commerce**, supportive of national economic security interests and responsive to Public Law and Executive direction, is responsible for promulgating Federal information technology and cybersecurity standards; regulating export of security technologies; representing U.S. industry on international trade policy and commercial data flow matters; security and privacy policies that apply to the Internet's domain name system; protecting intellectual property; conducting cybersecurity research and development; and assuring timely availability of industrial products, materials, and services to meet homeland security requirements.
- The **Secretary of Education** oversees discretionary grants and technical assistance to help schools plan for and respond to emergencies that disrupt teaching and learning. The Department of Education is a supporting Federal agency in the response and management of emergencies under the *National Response Framework*.
- The **Secretary of Energy** maintains stewardship of vital national security capabilities, from nuclear weapons to leading edge research and development programs. The Department of Energy (DOE) is the designated Federal agency to provide a unifying structure for the integration of Federal critical infrastructure and key resources protection efforts specifically for the Energy

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

Sector. It is also responsible for maintaining continuous and reliable energy supplies for the United States through preventive measures and restoration and recovery actions. DOE is the coordinator and primary agency for ESE #12 – Energy when incidents require a coordinated Federal response to facilitate the restoration of damaged energy systems and components.

- The **Administrator of the Environmental Protection Agency (EPA)** leads the EPA, which is charged with protecting human health and the environment. For certain incidents, EPA is the coordinator and primary agency for ESE #10 – Oil and Hazardous Materials Response, in response to an actual or potential discharge and/or uncontrolled release of oil or hazardous materials. EPA is the Sector-Specific Agency for securing the Water Sector.
- The **Secretary of Housing and Urban Development** is the coordinator and primary agency for ESE #14 – Long-Term Community Recovery, which provides a mechanism for coordinating Federal support to State, tribal, regional, and local governments, nongovernmental organizations (NGOs), and the private sector to enable community recovery from the long-term consequences of extraordinary disasters.
- The **Secretary of the Interior** develops policies and procedures for all types of hazards and emergencies that impact Federal lands, facilities, infrastructure, and resources; tribal lands; and insular areas. The Department of the Interior (DOI) is also a primary agency for ESE #9 – Search and Rescue, providing specialized lifesaving assistance to State, tribal, and local authorities when activated for incidents or potential incidents requiring a coordinated Federal response. DOI, together with the Department of Agriculture, also operates the National Interagency Fire Center.
- The **Secretary of Transportation** collaborates with DHS on all matters relating to transportation security and transportation infrastructure protection and in regulating the transportation of hazardous materials by all modes (including pipelines). The Secretary of Transportation is responsible for operating the national airspace system.
- **Other Federal Agencies** are also part of the homeland security enterprise and contribute to the homeland security mission in a variety of ways. This includes agencies with responsibilities for regulating elements of the Nation's critical infrastructure to assure public health, safety, and the common defense, developing and implementing pertinent public policy, supporting efforts to

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

assure a resilient homeland, and collaborating with those departments and agencies noted above in their efforts to secure the homeland.

- **Critical Infrastructure and Key Resource (CIKR) Owners and Operators** develop protective programs and measures to ensure that systems and assets, whether physical or virtual, are secure from and resilient to cascading, disruptive impacts. Protection includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links, including actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. CIKR owners and operators also prepare business continuity plans and ensure their own ability to sustain essential services and functions.
- **Major and Multinational Corporations** operate in all sectors of trade and commerce that foster the American way of life and support the operation, security, and resilience of global movement systems. They take action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. They contribute to developing the ideas, science, and technology that underlie innovation in homeland security. During times of disaster, they provide response resources (donated or compensated)—including specialized teams, essential service providers, equipment, and advanced technologies—through public-private emergency plans/partnerships or mutual aid and assistance agreements, or in response to requests from government and nongovernmental-volunteer initiatives.
- **Small Businesses** contribute to all aspects of homeland security and employ more than half of all private-sector workers. They support response efforts by developing contingency plans and working with local planners to ensure that their plans are consistent with pertinent response procedures. When small businesses can survive and quickly recover from disasters, the Nation and economy are more secure and more resilient. They perform research and development, catalyze new thinking, and serve as engines of innovation for development of new solutions to key challenges in homeland security.
- **Governors** are responsible for overseeing their State's threat prevention activities as well the State's response to any emergency or disaster, and take an active role in ensuring that other State officials and agencies address the range of homeland security threats, hazards, and challenges. During an emergency, Governors will play a number of roles, including the State's chief communicator

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

and primary source of information on the need for evacuations, the scope of the disaster, and the availability of assistance. Governors are commanders of their National Guards and are able to call them up to assist under State active duty during a disaster, and also retain command over their National Guard under Title 32 status. During a disaster, Governors also will need to make decisions regarding the declaration of emergencies or disasters, requests for mutual aid, and calls for Federal assistance.

- **State and Territorial Governments** coordinate the activity of cities, counties, and intrastate regions. States administer Federal homeland security grants to local and tribal (in certain grant programs) governments, allocating key resources to bolster their prevention and preparedness capabilities. State agencies conduct law enforcement and security activities, protect the Governor and other executive leadership, and administer State programs that address the range of homeland security threats, hazards, and challenges. States government officials lead statewide disaster and mitigation planning. During response, States coordinate resources and capabilities throughout the State and are responsible for requesting and obtaining resources and capabilities from surrounding States. States often mobilize these substantive resources and capabilities to supplement the local efforts before, during, and after incidents.
- **Tribal Leaders** are responsible for the public safety and welfare of their membership. They can serve as both key decisionmakers and trusted sources of public information during incidents.
- **Tribal Governments**, which have a special status under Federal laws and treaties, ensure the provision of essential services to members within their communities, and are responsible for developing emergency response and mitigation plans. Tribal governments may coordinate resources and capabilities with neighboring jurisdictions, and establish mutual aid agreements with other tribal governments, local jurisdictions, and State governments. Depending on location, land base, and resources, tribal governments provide law enforcement, fire, and emergency services as well as public safety to their members.
- **Mayors** and other local elected and appointed officials (such as city managers) are responsible for ensuring the public safety and welfare of their residents, serving as their jurisdiction's chief communicator and a primary source of information for homeland security-related information, and ensuring their governments are able to carry out emergency response activities. They serve as

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

both key decisionmakers and trusted sources of public information during incidents.

- **Local Governments** provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for all manner of hazards and emergencies. Through the Urban Areas Security Initiative (UASI) program, cities (along with counties in many cases) address multi-jurisdictional planning and operations, equipment support and purchasing, and training and exercises in support of high-threat, high-density urban areas. UASI grants assist local governments in building and sustaining homeland security capabilities. Local governments coordinate resources and capabilities during disasters with neighboring jurisdictions, NGOs, the State, and the private sector.
- **County Leaders** serve as chief operating officers of county governments, both rural and urban. This includes supporting and enabling the county governments to fulfill their responsibilities to constituents, including public safety and security. In some States, elected county officials such as sheriffs or judges also serve as emergency managers, search and rescue officials, and chief law enforcement officers.
- **County Governments** provide front-line leadership for local law enforcement, fire, public safety, environmental response, public health, and emergency medical services for all manner of hazards and emergencies. In many cases, county government officials participate in UASIs with other urban jurisdictions to assist local governments in building and sustaining capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism. County governments coordinate resources and capabilities during disasters with neighboring jurisdictions, NGOs, the State, and the private sector.
- The **American Red Cross** is a supporting agency to the mass care functions of ESF #6 -- Mass Care, Emergency Assistance, Housing, and Human Services under the NRE. As the Nation's largest mass care service provider, the American Red Cross provides sheltering, feeding, bulk distribution of needed items, basic first aid, welfare information, and casework, among other services, at the local level as needed. In its role as a service provider, the American Red Cross works closely with local, tribal, and State governments to provide mass care services to victims of every disaster, large and small, in an affected area.

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

- **National Voluntary Organizations Active in Disaster (National VOAD)** is a consortium of approximately 50 national organizations and 55 State and territory equivalents that typically send representatives to the Federal Emergency Management Agency's National Response Coordination Center to represent the voluntary organizations and assist in response coordination. Members of National VOAD form a coalition of nonprofit organizations that respond to disasters as part of their overall mission.
- **Nongovernmental Organizations (NGOs)** provide sheltering, emergency food supplies, counseling services, and other vital support services to support response and promote the recovery of disaster victims. They often provide specialized services that help individuals with special needs, including those with disabilities, and provide resettlement assistance and services to arriving refugees. NGOs also play key roles in engaging communities to integrate lawful immigrants into American society and reduce the marginalization or radicalization of these groups.
- **Communities** and community organizations foster the development of organizations and organizational capacity that act toward a common goal (such as Neighborhood Watch, Community Emergency Response Teams, or providing emergency food or shelter). These groups may possess the knowledge and understanding of the threats, local response capabilities, and special needs within their jurisdictions and have the capacity necessary to alert authorities of those threats, capabilities, or needs. Additionally, during an incident these groups may be critical in passing along vital incident communications to individuals and families, and to supporting critical response activities in the initial stages of a crisis.
- **Individuals and Families** take the basic steps to prepare themselves for emergencies, including understanding the threats and hazards that they may face, reducing hazards in and around their homes, preparing an emergency supply kit and household emergency plans (that include care for pets and service animals), monitoring emergency communications carefully, volunteering with established organizations, mobilizing or helping to ensure community preparedness, enrolling in training courses, and practicing what to do in an emergency. These individual and family preparedness activities strengthen community resilience and mitigate the impact of disasters. In addition, individual vigilance and awareness can help communities remain safer and bolster prevention efforts.

## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

Figure A-1. Emergency Support Functions and ESF Coordinators  
(Source: National Response Framework)

<b>ESF #1 – Transportation</b> <b>ESF Coordinator: Department of Transportation</b> <ul style="list-style-type: none"> <li>• Aviation/airspace management/control</li> <li>• Transportation safety</li> <li>• Restoration and recovery of transportation infrastructure</li> <li>• Movement restrictions</li> <li>• Damage and impact assessments</li> </ul>	<b>ESF #8 – Public Health and Medical Services</b> <b>ESF Coordinator: Department of Health and Human Services</b> <ul style="list-style-type: none"> <li>• Public health</li> <li>• Medical</li> <li>• Mental health services</li> <li>• Mass fatality management</li> </ul>
<b>ESF #2 – Communications</b> <b>ESF Coordinator: DHS (National Communications System)</b> <ul style="list-style-type: none"> <li>• Coordination with telecommunications and information technology industries</li> <li>• Restoration and repair of telecommunications infrastructure</li> <li>• Protection, restoration, and sustainment of national cyber and information technology resources</li> <li>• Oversight of communications within the Federal incident management and response structures</li> </ul>	<b>ESF #9 – Search and Rescue</b> <b>ESF Coordinator: DHS (FEMA)</b> <ul style="list-style-type: none"> <li>• Life-saving assistance</li> <li>• Search and rescue operations</li> </ul>
<b>ESF #3 – Public Works and Engineering</b> <b>ESF Coordinator: Department of Defense (USACE)</b> <ul style="list-style-type: none"> <li>• Infrastructure protection and emergency repair</li> <li>• Infrastructure restoration</li> <li>• Engineering services and construction management</li> <li>• Emergency contracting support for life-saving and life-sustaining services</li> </ul>	<b>ESF #10 – Oil and Hazardous Materials Response</b> <b>ESF Coordinator: Environmental Protection Agency</b> <ul style="list-style-type: none"> <li>• Oil and hazardous materials response</li> <li>• Environmental short- and long-term cleanup</li> </ul>
<b>ESF #4 – Firefighting</b> <b>ESF Coordinator: Department of Agriculture (U.S. Forest Service)</b> <ul style="list-style-type: none"> <li>• Coordination of Federal firefighting activities</li> <li>• Support to wildland, rural, and urban firefighting operations</li> </ul>	<b>ESF #11 – Agriculture and Natural Resources</b> <b>ESF Coordinator: Department of Agriculture</b> <ul style="list-style-type: none"> <li>• Nutrition assistance</li> <li>• Animal and plant disease and pest response</li> <li>• Food safety and security</li> <li>• Natural and cultural resources and historic properties protection</li> <li>• Safety and well-being of household pets</li> </ul>
<b>ESF #5 – Emergency Management</b> <b>ESF Coordinator: DHS (FEMA)</b> <ul style="list-style-type: none"> <li>• Coordination of incident management and response efforts</li> <li>• Issuance of mission assignments</li> <li>• Resource and human capital</li> <li>• Incident action planning</li> <li>• Financial management</li> </ul>	<b>ESF #12 – Energy</b> <b>ESF Coordinator: Department of Energy</b> <ul style="list-style-type: none"> <li>• Energy infrastructure assessment, repair, and restoration</li> <li>• Energy industry utilities coordination</li> <li>• Energy forecast</li> </ul>
<b>ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services</b> <b>ESF Coordinator: DHS (FEMA)</b> <ul style="list-style-type: none"> <li>• Mass care</li> <li>• Emergency assistance</li> <li>• Disaster housing</li> <li>• Human services</li> </ul>	<b>ESF #13 – Public Safety and Security</b> <b>ESF Coordinator: Department of Justice</b> <ul style="list-style-type: none"> <li>• Facility and resource security</li> <li>• Security planning and technical resource assistance</li> <li>• Public safety and security support</li> <li>• Support to access, traffic, and crowd control</li> </ul>
<b>ESF #7 – Logistics Management and Resource Support</b> <b>ESF Coordinator: General Services Administration and DHS</b> <ul style="list-style-type: none"> <li>• Comprehensive, national incident logistics planning, management, and sustainment capability</li> <li>• Resource support (facility space, office equipment and supplies, contracting services, etc.)</li> </ul>	<b>ESF #14 – Long-Term Community Recovery</b> <b>ESF Coordinator: DHS (FEMA)</b> <ul style="list-style-type: none"> <li>• Social and economic community impact assessment</li> <li>• Long-term community recovery assistance to States, tribes, local governments, and the private sector</li> <li>• Analysis and review of mitigation program implementation</li> </ul>
	<b>ESF #15 – External Affairs</b> <b>ESF Coordinator: DHS</b> <ul style="list-style-type: none"> <li>• Emergency public information and protective action guidance</li> <li>• Media and community relations</li> <li>• Congressional and international affairs</li> <li>• Tribal and insular affairs</li> </ul>



## APPENDIX A: ROLES AND RESPONSIBILITIES ACROSS THE HOMELAND SECURITY ENTERPRISE

Figure A-2. Sector-Specific Agencies  
(Source: National Infrastructure Protection Plan)

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture (a) Department of Health and Human Services(b)	Agriculture and Food
Department of Defense (c)	Defense Industrial Base
Department of Energy	Energy (d)
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water (e)
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste Government Facilities (f)
Federal Protective Service	
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration U.S. Coast Guard (h)	Transportation Systems (g)

- a The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).
- b The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.
- c Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President as Commander in Chief to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
- d The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.
- e The Water Sector includes drinking water and wastewater systems.
- f The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.
- g As stated in Homeland Security Presidential Directive 7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.
- h The U.S. Coast Guard is the SSA for the maritime transportation mode.

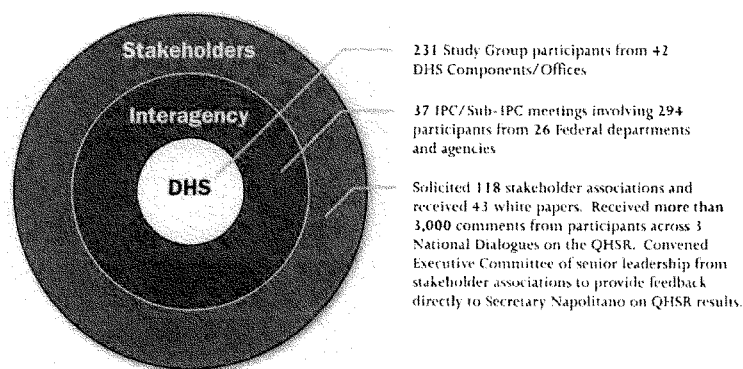
## APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

### *Review Approach: Engagement Through Transparency and Collaboration*

Section 2401 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* amends Title VII of the *Homeland Security Act of 2002* to require the Secretary of Homeland Security to conduct a Quadrennial Homeland Security Review (QHSR) every 4 years beginning in 2009. In doing so, the Department of Homeland Security (DHS) was directed to consult with (A) the heads of other Federal agencies, including the Attorney General, the Secretary of State, the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of the Treasury, the Secretary of Agriculture, and the Director of National Intelligence; (B) key officials of the Department; and (C) other relevant governmental and nongovernmental entities, including State, local, and tribal government officials, Members of Congress, private-sector representatives, academics, and other policy experts.

As noted in the QHSR report, homeland security is a distributed and diverse national enterprise. The term “enterprise” refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners -- as well as individuals, families, and communities -- to maintain critical homeland security capabilities. It recognizes the diverse risks, needs, and priorities of these different stakeholders, and connotes a broad-based community with a common interest in the public safety and well-being of America and American society. Substantive and consistent engagement of stakeholders across the enterprise was therefore a requirement of conducting the first QHSR.

**Figure B-1. Constituency Participation in the QHSR**



## APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

In preparing the QHSR, the Department has benefited from the constructive engagement of thousands of dedicated individuals from across the country and, indeed, around the globe, including the key officials of DHS, the heads of other Federal agencies, and other relevant governmental and nongovernmental entities, including State, local, tribal, and territorial governments, as well as the broader public at large. Although numbers alone cannot capture the depth and vibrancy of the debates and discussions that occurred throughout the process of preparing the QHSR, the last 8 months engaged more than 100 stakeholder associations and more than 500 experts from government at all levels, as well as academia and the private sector. Our online National Dialogues had over 20,000 visits, with over 3,000 comments submitted.

### *Department of Homeland Security*

The core of the QHSR approach was the formation of seven study groups that consisted of representatives from across DHS. The study groups were each led by a DHS official and facilitated by an independent subject-matter expert, both of whom ensured that all viewpoints were aired and that divergent opinions were brought forward. Consensus was not the object of the study group process; rather, it was to define the nature and purpose of the homeland security missions, describe the primary national tools required to enable those missions, *and identify and bring forward any major divergent points of view regarding the mission areas or national tools*. Specifically, the mission area study groups defined major goals, objectives, and key strategic outcomes for each of the homeland security mission areas. Three additional study groups examined homeland security national risk assessment, homeland security planning and capabilities, and DHS strategic management.

- **Study Groups:** In keeping with the inclusive approach of the review, over 200 participants from 42 DHS directorates, components, and offices made up the bulk of the study groups. The work of the DHS study group participants was supported by 35 subject-matter experts and research analysts from the Homeland Security Studies and Analysis Institute (HSSAI), the Department's federally funded research and development center. The study groups conducted their analysis over a 5-month period, with work products being consistently shared with the other stakeholder groups via different collaboration processes.
- **Steering Committee:** A Steering Committee, chaired by the Deputy Assistant Secretary for Policy (Strategic Plans) and composed of the DHS leads and independent facilitators of each of the study groups, as well as the Director of Program Analysis and Evaluation and representatives from the DHS Office of Intergovernmental Affairs, the Science and Technology Directorate, the Office of International Affairs, the Office of General Counsel, and the Office of

## APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

Intelligence and Analysis, convened weekly in person and by teleconference to ensure integration and consistency across the various studies. In addition, the Steering Committee held formal monthly in-progress reviews, during which each study group presented its progress towards developing its recommendations and brought forward unresolved questions and issues that required leadership consideration and decision.

- **DHS Senior Leadership Meetings:** More than a dozen DHS Deputy Secretary-led senior leadership meetings were held at the end of the study group deliberation period to review and concur on study group recommendations. Final decisions on the recommendations reflected departmental acknowledgement of the major themes around which the QHSR report was written.

### *Other Federal Departments and Agencies*

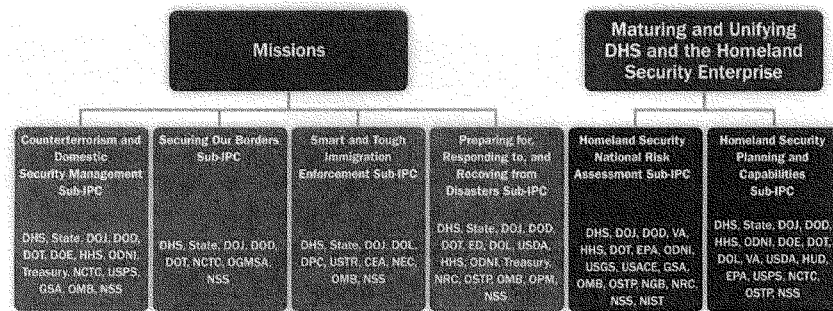
DHS engaged with the White House National Security Staff to ensure robust interagency engagement and involvement with the QHSR. Specifically, interagency input was garnered through the following:

- **Sub-Interagency Policy Committees (Sub-IPCs):** Six special sub-IPCs were established by the National Security Staff to align with six of the QHSR study groups (the seventh study group, on DHS Strategic Management, was internally focused on DHS and therefore did not require a special sub-IPC) (see Figure B-2). The sub-IPCs were not venues for interagency *decisionmaking* on key issues; rather, they provided a forum for study groups to gather interagency input as study group content was developed. Over the course of the review, study groups held over 35 meetings that included approximately 294 Federal participants from 26 Federal departments and agencies through the special sub-IPCs, thereby ensuring interagency perspectives were solicited and represented in final study group recommendations.
- **Strategy Coordination Group:** In addition to the sub-IPCs, a special interagency Strategy Coordination Group was created to provide strategy and policy planners from across the interagency community an opportunity to share their feedback and perspectives on the review. Meeting monthly, the forum also allowed participants to identify issues being raised across multiple, similar strategic reviews and to share lessons learned and best practices on their respective reviews and planning processes.

## APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

- **Interagency Processes:** The final QHSR report required vetting by interagency principals prior to delivery to Congress. Several Deputies Committee meetings were convened by the National Security Staff to discuss QHSR findings prior to the formal Office of Management and Budget (OMB) clearance process, allowing DHS to address major concerns before final interagency review. The OMB review process allowed Federal departments and agencies to formally comment on the QHSR report.

Figure B-2. Sub-Interagency Policy Committees and Interagency Participation



### Congressional Engagement

Congressional engagement began during the preparatory phases of the QHSR and continued throughout the study period. DHS submitted an initial QHSR Resource Plan to Congress in early 2008, and the Deputy Assistant Secretary for Policy (Strategic Plans) testified before the House Homeland Security Committee, Subcommittee on Management, Investigations, and Oversight in July 2008. The DHS Office of Policy, together with the DHS Office of Program Analysis and Evaluation, also briefed staff from the House Homeland Security Committee, the Senate Homeland Security and Government Affairs Committee, and the House and Senate Appropriations Subcommittees on Homeland Security in 2008 regarding QHSR preparations.

In 2009, the DHS Office of Policy, together with the DHS Office of Program Analysis and Evaluation, conducted 17 briefings to congressional staff on QHSR status and process, including multiple briefings to staff from the House Homeland Security Committee, the Senate Homeland Security and Government Affairs Committee, and the House and Senate Appropriations Subcommittees on Homeland

## APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS

Security, as well as briefings to staff from the House Energy and Commerce Committee, the House Judiciary Committee, the House Transportation and Infrastructure Committee, the Senate Commerce Committee, and the Senate Judiciary Committee.

### *State, Local, Tribal, and Territorial Partners and Other Stakeholders*

Several mechanisms were established to ensure the broadest possible outreach to critical State, local, and tribal partners as well as the general public.

- **Stakeholder Call for Comment:** The Secretary of Homeland Security began the QHSR study period with a letter to 118 homeland security stakeholder organizations representing State, local, tribal, territorial, nongovernmental, private-sector, and professional interests having roles and responsibilities in homeland security activities, inviting these organizations to submit papers and other materials relating to the QHSR study areas. Over 40 position papers were received and disseminated to study groups, and these papers helped to frame and inform the deliberations of the study groups. This *early engagement* of homeland security stakeholders at the beginning of the review process was a critical element of the QHSR.
- **National Dialogue on the QHSR:** *Sustained engagement* of the stakeholder community was another critical element of the QHSR. In a groundbreaking initiative, DHS held three online, collaborative “National Dialogue on the QHSR” sessions to capture the direct input and perspectives of a wide array of participants in the homeland security enterprise. Each National Dialogue presented study group materials that were posted for a period of 7 to 10 days for dialogue participants to rate and provide comment. The National Dialogues were open to anyone who wanted to provide input on QHSR content, although the Department engaged in deliberate outreach to several hundred organizations with interests in homeland security. Over the course of 3 dialogues, more than 20,000 visits were logged, resulting in over 3,000 comments on study group material. National Dialogue comments and content ratings were provided to the study groups who used the information to inform their iterative deliberations throughout the analytic period of the review. Revised study group materials were posted on each subsequent dialogue, demonstrating how materials evolved over the course of the review and showing participants how their comments informed study group work.
- **Executive Committee:** It would not have been possible to meaningfully convene representatives from all individual States, counties, cities, tribes, and territories to discuss QHSR findings. Therefore, DHS invited the leadership of

## **APPENDIX B: QUADRENNIAL HOMELAND SECURITY REVIEW PROCESS**

10 key stakeholder associations that are broadly representative of State, local, tribal, and territorial governments to form the “virtual” QHSR Executive Committee. The Executive Committee consisted of the leaders of the following organizations: the National Governors Association, the Council of State Governments, the U.S. Conference of Mayors, the National League of Cities, the National Association of Counties, the National Council of State Legislatures, the National Congress of American Indians, the International City/County Management Association, the National Emergency Management Association, and the International Association of Emergency Managers. DHS held monthly teleconferences with the participating organizations throughout the analytic phase of the review to keep these organizations appraised of review progress. These organizations also participated in the collaborative events DHS held throughout the review, such as the Secretary’s call for comment at the beginning of the review and the three National Dialogue sessions. Finally, on November 19, 2009, the Secretary of Homeland Security met in person with leadership representatives of the Executive Committee organizations to share key findings and recommendations of the QHSR. This in-person meeting provided key stakeholder associations the opportunity to comment on QHSR findings and recommendations in a similar manner to, and at a similar time as, Federal department and agency leadership.

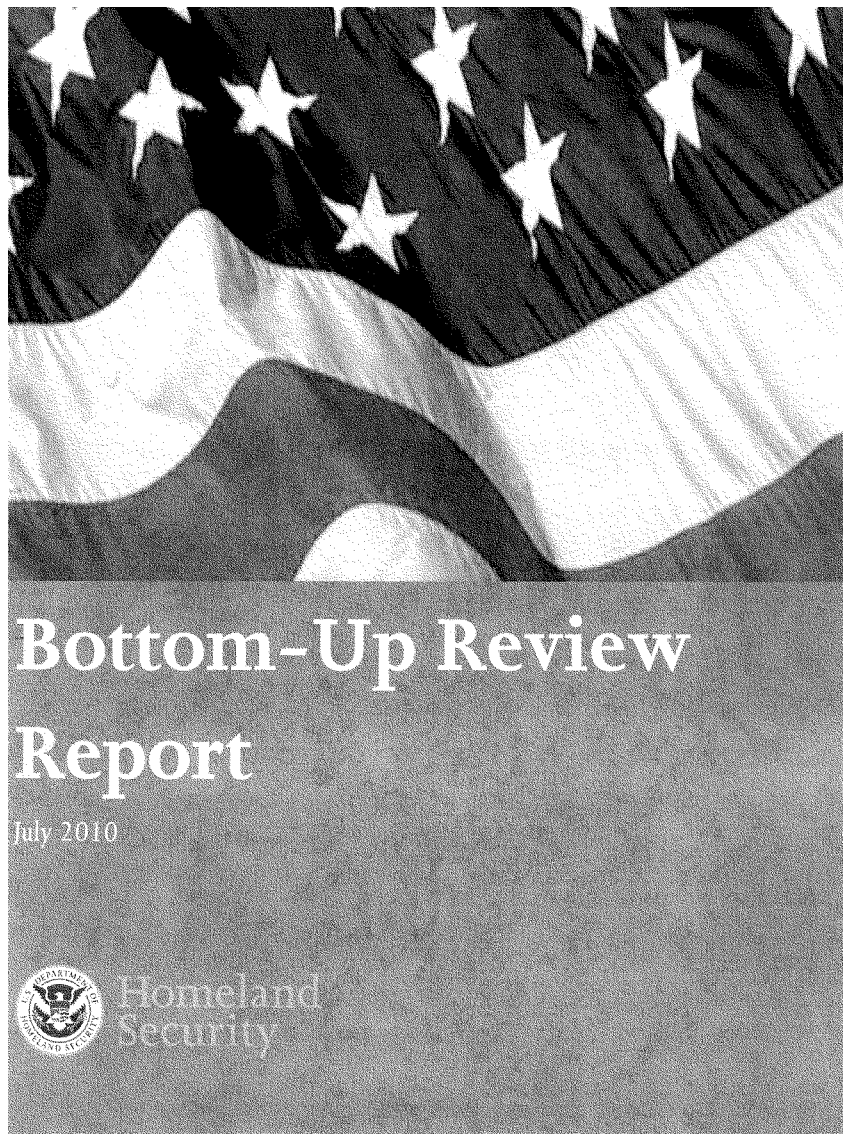
**APPENDIX C: ACRONYM LIST**

CBRN	Chemical, Biological, Radiological, and Nuclear
CEA	Council of Economic Advisors
CERT	Community Emergency Response Team
CIKR	Critical Infrastructure and Key Resource
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
DPC	Domestic Policy Council
ED	Department of Education
EPA	Environmental Protection Agency
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
GSA	General Services Administration
HHS	Department of Health and Human Services
HSSAI	Homeland Security Studies and Analysis Institute
HUD	Department of Housing and Urban Development
IC	Intelligence Community
IPC	Interagency Policy Committee
NCTC	National Counterterrorism Center
NEC	National Economic Council
NGB	National Guard Bureau
NGO	Nongovernmental Organization
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology



**APPENDIX C: ACRONYM LIST**

NRC	Nuclear Regulatory Commission
NRF	National Response Framework
NSS	National Security Strategy
ODNI	Office of the Director of National Intelligence
OGMSA	Office of Global Maritime Situational Awareness
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
QHSR	Quadrennial Homeland Security Review
SSA	Sector-Specific Agency
UASI	Urban Areas Security Initiative
USACE	U.S. Army Corps of Engineers
USDA	Department of Agriculture
USGS	U.S. Geological Survey
USPS	U.S. Postal Service
USTR	U.S. Trade Representative
VA	Department of Veterans Affairs
[National] VOAD	Voluntary Organizations Active in Disaster
WMD	Weapon(s) of Mass Destruction



### Table of Contents

Secretary's Letter .....	iii
Preface.....	v
Executive Summary .....	vii
I. Introduction .....	1
II. The Mission of the Department of Homeland Security .....	3
III. Enhancing Mission Performance .....	4
A. Preventing Terrorism and Enhancing Security .....	4
Current Authorities .....	4
Overview of the DHS Role .....	5
Preventing Terrorist Attacks .....	6
Preventing Unauthorized Acquisition and Use of Chemical, Biological, Radiological, and Nuclear (CBRN) Materials and Capabilities .....	7
Managing Risks to Critical Infrastructure, Key Leadership, and Events ....	7
Initiatives and Enhancements .....	8
B. Securing and Managing our Borders.....	12
Current Authorities .....	12
Overview of the DHS Role .....	12
Effectively Controlling U.S. Air, Land, and Sea Borders .....	13
Safeguarding Lawful Travel and Trade .....	14
Disrupting and Dismantling Transnational Criminal Organizations .....	15
Initiatives and Enhancements .....	16
C. Enforcing and Administering our Immigration Laws .....	18
Current Authorities .....	18
Overview of the DHS Role .....	18
Strengthening and Effectively Administering the Immigration System.....	18
Preventing Unlawful Immigration .....	19
Initiatives and Enhancements .....	20
D. Safeguarding and Securing Cyberspace.....	23
Current Authorities .....	23
Overview of the DHS Role .....	23
Creating a Safe, Secure, and Resilient Cyber Environment .....	23

Promoting Cybersecurity Knowledge and Innovation.....	25
Initiatives and Enhancements .....	26
E. Ensuring Resilience to Disasters .....	27
Current Authorities .....	27
Overview of the DHS Role .....	28
Mitigating Hazards.....	29
Enhancing Preparedness .....	29
Ensuring Effective Emergency Response .....	29
Supporting Community Recovery .....	30
Initiatives and Enhancements .....	31
F. Complementary Departmental Responsibilities and Hybrid Capabilities .....	33
IV. Improving Department Management.....	33
The DHS Efficiency Review .....	33
A DHS International Engagement Framework.....	33
Initiatives and Enhancements .....	34
V. Increasing Accountability .....	37
Data and Performance Management.....	37
Congressional Accountability .....	38
Initiatives and Enhancements .....	38
VI. Conclusion .....	39
Annex A: DHS Component Composition	
Annex B: A Day in the Life of the Department of Homeland Security	
Annex C: The DHS Efficiency Review	
Annex D: Alignment of Major DHS Programs to Homeland Security Missions	
Annex E: Sector-Specific Agencies	
Annex F: Congressional Oversight of DHS in the 110th Congress	

Secretary

U.S. Department of Homeland Security  
Washington, DC 20528

# Homeland Security

In February 2010, the Department of Homeland Security published our Nation's first ever comprehensive review of America's strategy for homeland security—the Quadrennial Homeland Security Review (QHSR). The QHSR was the first step in setting forth the strategic path forward to guide the activities of the homeland security enterprise toward a common end: a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive. The QHSR accomplished this by laying out a vision for a secure homeland, key mission priorities, and specific goals for each of those mission areas. The QHSR is consistent with, and expands upon, the recently-released *National Security Strategy*.

At the same time, the QHSR and the bottom-up review (BUR) processes reflect the enormity of the ongoing challenge of building OneDHS from previously separate organizations and entities. The QHSR and BUR processes intentionally challenge us to consider difficult questions regarding the mission, organization, and priorities of homeland security. Forging a single integrated and optimized Department out of components extracted from previously fully-formed and functioning agencies has been a great challenge for every leadership team at DHS since its founding.

The QHSR identified five core mission areas of homeland security—preventing terrorism and enhancing security, securing and managing our borders, enforcing and administering our immigration laws, safeguarding and securing cyberspace, and ensuring resilience to disasters. These missions, and the associated goals defined in the QHSR, comprise the backbone of what it takes to keep America safe, secure, and resilient. The QHSR was a first and essential step of a multi-step process to answer key questions regarding what must be done to accomplish the missions of homeland security. The underlying premise of the BUR was the need to also examine programs, plans, structures, and resources from the bottom up.

The BUR provides the results of an unprecedented Department-wide assessment of DHS, begun in November 2009, to align the Department's programmatic activities and organizational structure with the mission sets and goals identified in the QHSR. The BUR report focuses on the following questions:

- How can we strengthen the Department's performance in each of the five mission areas?
- How should we improve Departmental operations and management?

- How can we increase accountability for the resources entrusted to DHS?

The BUR will serve as a road map for these questions. First and foremost, it provides direction for reinforcing the cornerstone of homeland security: preventing terrorism. The BUR also focuses on combating cybersecurity threats, ensuring resilience to all hazards, and the critical need to reform our immigration system. It also provides new emphasis on the importance of enhancing the security and resilience of the global systems that are responsible for the movement of people and goods across our borders. Finally, the review lays a foundation for improving Departmental operations and management and increasing accountability for the resources entrusted to DHS.

I am very proud of the work done every day by the men and women in the Department of Homeland Security as well as the hundreds of thousands of Federal, State, local, tribal, and territorial officials, private citizens, and businesses with whom we partner to keep America safe, secure, and resilient. We have accomplished much and have much more to accomplish together in the years ahead. The QHSR and the results of the BUR in this report will guide these important efforts.

Secretary Janet Napolitano

## Preface

In 2007, the Homeland Security Act of 2002 was amended to require the Department of Homeland Security (DHS) to initiate implementation of a Quadrennial Homeland Security Reviews (QHSR) in 2009, and to conduct subsequent reviews every four years thereafter. The purpose of the QHSR was to describe the threats to the national security interests of the Nation, outline and prioritize the full range of homeland security missions, and update the national homeland security strategy. It would also assess the alignment of the Department to the strategy, promote mechanisms for turning strategic requirements into an acquisition strategy and expenditure plan, and identify the budget plan for successfully executing the homeland security missions.

DHS conducted the first QHSR in 2009, and delivered the QHSR Report to Congress on February 1, 2010. The QHSR was a comprehensive examination of the homeland security strategy of the Nation and included recommendations regarding the long-term strategy and priorities of the Nation for homeland security. The QHSR Report included the results of the QHSR, a national homeland security strategy, a description of the critical homeland security missions of the Nation, and an explanation of the underlying assumptions used in conducting the review. The QHSR is consistent with, and expands upon, the recently-released *National Security Strategy*.

A bottom-up review (BUR) of the Department of Homeland Security was initiated in November 2009 as an immediate follow-on and complement to the QHSR. The BUR included an assessment of the organizational alignment of the Department with the homeland security missions set forth in the QHSR, including the Department's organizational structure, management systems, procurement systems, and physical and technical infrastructure. The BUR also included a review and assessment of the effectiveness of the mechanisms of the Department for turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan within the Department.

The BUR resulted in a comprehensive catalogue of DHS activities across the homeland security missions, as well as a list of over 300 potential initiatives and enhancements. The BUR Report distills the results of this analysis, describing the alignment of the Department with the homeland security missions, and setting forth the Department's priority initiatives and enhancements to increase mission performance, improve Departmental management, and increase accountability over the next four years. The BUR Report includes recommendations for improving the organizational alignment of the Department and enhancing its business processes.

The BUR is the second step of a three-step process. The Department's FY 2012 budget request will begin the process of implementing the BUR initiatives and enhancements, and the corresponding FY 2012-2016 Future Years Homeland Security Program will set forth the budget plan required to provide sufficient resources to successfully execute the Department's responsibilities across the full range of homeland security missions as described in the QHSR, with a priority placed on the initiatives and enhancements set forth in the BUR Report. As such, the BUR Report is not a budget request and does not describe specific budget requests for FY 2012 or for subsequent years. Nor is the BUR Report a strategic plan. Consequently, it neither

includes performance measures nor attaches resources to strategic goals and objectives, nor does it describe the sequence in which DHS will seek to implement the initiatives and enhancements described herein. Instead, the BUR Report sets forth DHS's conclusions concerning the priority initiatives and enhancements necessary to strengthen existing programs and address priority capability and capacity gaps over the FY 2012-2016 period, in order to set a foundation for future success.



### Executive Summary

The Department of Homeland Security (DHS) was formed in the wake of the terrorist attacks of September 11, 2001, as part of a deliberate and determined national effort to safeguard the United States against terrorism. DHS became the third-largest Federal department, bringing together 22 different Federal agencies, each with a role in this effort. Integrating these many disparate entities—some with long histories of independent or autonomous operations, and all with distinct operational cultures—while maintaining their unique strengths and capabilities has presented significant public policy and management challenges.

The submission of the Quadrennial Homeland Security Review (QHSR) Report to Congress on February 1, 2010 marked an important first step in a multi-step process to examine and address fundamental issues that concern homeland security. The QHSR Report described the Nation's homeland security interests, identified the critical homeland security missions, and defined a strategic approach to those missions by laying out the principal goals, essential objectives, and key strategic outcomes necessary for that approach to succeed. A bottom-up review (BUR) of the Department of Homeland Security was initiated in November 2009 as an immediate follow-on and complement to the congressionally mandated QHSR with the aim to align the Department's programmatic activities and organizational structure with the broader mission sets and goal identified in the QHSR. This report reflects that endeavor and represents an intermediate step between the QHSR Report and the DHS FY 2012-2016 Future Years Homeland Security Program (FYHSP), which will propose specific programmatic adjustments based on the QHSR strategic framework. Together, these three elements—the QHSR, the BUR, and the DHS FY 2012-2016 FYHSP—will address the primary legislative requirements set forth in Section 707 of the Homeland Security Act.

The aims of the BUR were several-fold: first, to gauge how well current activities and departmental organization align with mission priorities and goals as outlined in the QHSR; second, to identify ways to achieve better programmatic and budgetary alignment across the entire department; third, to identify areas for enhanced mission performance; and fourth, to prioritize initiatives to strengthen existing programs and organization, address shortfalls, and establish a foundation for innovation and advancement. DHS conducted extensive analysis of its current activities and organization in light of the mission goals and objectives set forth in the QHSR Report. The BUR Report describes DHS's current activities within each of the homeland security missions based on current authorities and roles and responsibilities, and sets forth DHS's conclusions concerning the priority initiatives and enhancements necessary to strengthen existing programs, address shortfalls, and set a foundation for future success.

While the robust portfolio of DHS's component agencies cannot be completely represented, this report briefly discusses the Department's core role in each of the homeland security missions, considers the additional statutory responsibilities of DHS component agencies, and outlines enhancements and initiatives that address three principal areas of emphasis:

- **Strengthen and Mature DHS**—There is a need to strengthen the Department's ability to execute its mission responsibilities, run itself, and account for the resources that have been entrusted to it.

- Enhance Partner Capability and Capacity—Responsibilities for homeland security are broader than those of DHS and indeed broader than those of the Federal government. For that reason, there is a need to strengthen the ability of partners in the homeland security enterprise—in particular, State, local, tribal, and territorial governments, and the private sector—to execute important aspects of core homeland security mission activities.
- Deepen International Engagement—Security of our homeland begins far from our shores. We must work with key international partners to improve the critical partnerships and activities that affect the homeland security mission space, consistent with the broad range of U.S. Government international priorities and in consultation and coordination with the Department of State and the U.S. Chiefs of Mission stationed in foreign countries.

DHS used three criteria to evaluate initiatives and identify enhancements:

- Does the initiative offer the opportunity to advance the safety, security, and resilience of the homeland beyond incremental improvements to current activities?
- Is the initiative sufficiently defined to permit the identification of performance objectives, measures, and targets?
- Can the initiative be achieved within the FY 2012-2016 timeframe?

#### **Mission 1: Preventing Terrorism and Enhancing Security**

Protecting the United States and its people from terrorism is the cornerstone of homeland security. DHS shares leadership roles and responsibilities in the U.S. government's efforts to prevent terrorist attacks with several Federal departments and agencies. DHS's responsibilities focus on three goals: preventing terrorist attacks; preventing the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear (CBRN) materials and capabilities within the United States; and reducing the vulnerability of critical infrastructure, key leadership, and events to terrorist attacks and other hazards. To improve performance in this mission area, the Department will:

- Strengthen counterterrorism coordination across DHS;
- Strengthen aviation security by bolstering the international aviation security system, improving security processes and technologies, and encouraging partnerships with industry;
- Create an integrated Departmental information sharing architecture and link that architecture to interagency efforts to prevent terrorism while protecting privacy, civil rights and civil liberties;
- Deliver infrastructure protection and resilience capabilities to the field, in conjunction with efforts to "design in" greater resilience in critical infrastructure;

- Set national performance standards for identification verification;
- Increase efforts to detect and counter nuclear and biological weapons and dangerous materials;
- Standardize and institutionalize the National Fusion Center Network;
- Promote safeguards for access to secure areas in critical facilities, including through increased risk-informed screening and recurrent vetting;
- Establish DHS as a center for excellence for canine training and deployment; and
- Redesign the Federal Protective Service to better match mission requirements.

#### **Mission 2: Securing and Managing Our Borders**

We are responsible for secure, well-managed borders that not only protect the United States against threats from abroad, but also expedite the safe flow of lawful travel and commerce. Achieving this outcome rests on three interrelated goals: effectively securing U.S. air, land, and sea borders; safeguarding lawful trade and travel; and disrupting and dismantling transnational criminal and terrorist organizations. To strengthen efforts to achieve these goals, the Department will:

- Expand joint operations and intelligence capabilities, including enhanced domain awareness;
- Enhance the security of the global trade and travel systems responsible for the secure movement of people and goods, including enhanced container and maritime security and prioritization of immigration and customs investigations relating to global trade and travel systems;
- Strengthen and expand DHS-related security assistance internationally (e.g. border integrity and customs enforcement security assistance) consistent with U.S. government security and foreign assistance objectives in consultation and coordination with the Departments of State and Defense; and
- Work closely with the governments of Canada and Mexico to enhance North American security.

#### **Mission 3: Enforcing and Administering Our Immigration Laws**

Smart and effective enforcement and administration of our immigration laws allows the government to facilitate lawful immigration while identifying and removing those who violate our laws. To support this mission area, DHS will:

- Pursue comprehensive immigration reform;
- Strengthen and improve the Department's immigration services process;
- Prioritize national security and fraud detection vetting in immigration services processes;
- Target egregious employers who knowingly exploit illegal workers;
- Dismantle human smuggling organizations through concerted law enforcement activity;
- Improve the detention and removal process by increasing non-investigatory law enforcement staffing and expanding Secure Communities and the Criminal Alien Program;
- Work with new Americans so that they fully transition to the rights and responsibilities of citizenship; and
- Build and maintain a model immigration detention system.

#### **Mission 4: Safeguarding and Securing Cyberspace**

Cyber infrastructure forms the backbone of the Nation's economy and connects every aspect of our way of life. While the cyber environment offers the potential for rapid technological advancement and economic growth, a range of malicious actors may seek to exploit cyberspace for dangerous or harmful purposes, disrupt communications or other services, and attack the Nation's infrastructure through cyber means. By statute and Presidential directive, DHS has the lead for the Federal government to secure civilian government computer systems, works with industry to defend privately-owned and operated critical infrastructure, and works with State, local, tribal and territorial governments to secure their information systems. In pursuing these initiatives and enhancements to strengthen the Department's capabilities in cybersecurity, DHS will:

- Better integrate and focus DHS cybersecurity and infrastructure resilience operations;
- Strengthen DHS ability to protect cyber networks;
- Increase predictive, investigative, and forensic capabilities for cyber intrusions and attacks; and
- Promote cybersecurity public awareness through the cyber awareness program and the planned implementation of a national public awareness and education campaign.

#### **Mission 5: Ensuring Resilience to Disasters**

Ensuring domestic resilience to disasters is grounded in the four fundamental elements of emergency management: mitigating hazards, increasing our Nation's preparedness, effectively

responding to emergencies, and supporting community recovery. During domestic disasters, the Department's role, largely executed through the Federal Emergency Management Agency (FEMA), is principally one of coordinator, working closely with our State, local, regional, tribal, and territorial partners, as well as nongovernmental organizations and the private sector, to enhance preparedness, build and sustain capabilities, and act as an aggregator of resources from across the Federal government. DHS, through FEMA, also has specific direct responsibilities, including disaster response and field coordination, disaster logistics, individual and public assistance programs, as well as national continuity programs. DHS maintains a significant first responder capability for disasters in the maritime domain through the U.S. Coast Guard (USCG), and also ensures the resilience of critical infrastructure to disasters through the National Protection and Programs Directorate. In order to strengthen mission performance, DHS will:

- Enhance catastrophic disaster preparedness at the Federal, State, local, tribal, and territorial levels, as well as within nongovernmental organizations and the private sector, through nationally agreed-upon, risk-based preparedness standards;
- Improve the capabilities of DHS to lead in emergency management through a new strategic approach to developing FEMA's workforce, creating an emergency management career path, and harmonizing first responder training across DHS;
- Explore opportunities with the private sector to "design-in" greater resilience for critical infrastructure; and
- Make individual and family preparedness and critical facility resilience inherent in community preparedness.

#### **Complementary Department Responsibilities and Hybrid Capabilities**

DHS also performs a number of services and functions that are complementary to its homeland security mission responsibilities, including marine safety, stewardship, and environmental protection, and certain categories of law enforcement activities. These services and functions are typically performed with hybrid capabilities—assets and resources capable of performing multiple missions—which are a hallmark of homeland security. For example, the same assets and personnel that patrol our borders, enforce our immigration laws, and respond to major oil spills also enforce safety regulations, assist travelers, and safeguard natural resources. These complementary activities are critical to fulfilling other national interests and are often intertwined with and mutually supporting of homeland security activities.

#### **Improving Department Management**

The integration of 22 different Federal departments and agencies into a unified, integrated Department of Homeland Security continues to represent a significant public policy and management challenge. Over the course of its brief history, DHS has evolved to its current structure, which includes seven operating components, four headquarters directorates, and over 15 additional supporting offices, many of which combine responsibilities for policy,

management, operations, acquisition, external affairs, and research and development. In order to improve department management, DHS proposes to:

- Seek restoration of the Secretary's reorganizational authority for DHS headquarters to address new threats and realize greater efficiencies;
- Realign component regional configurations into a single DHS regional structure;
- Improve cross-Departmental management, policy, and functional integration;
- Strengthen DHS internal counterintelligence capabilities and internal intelligence sharing and distribution;
- Enhance the Department's risk management capability;
- Invest in the DHS workforce and improve retention and morale by strengthening employee health and wellness programs;
- Strengthen coordination within DHS through cross-Departmental training and career paths;
- Increase diversity in the DHS workforce, especially at senior levels; and
- Balance the DHS workforce by ensuring strong federal control of all DHS work and reducing reliance on contractors as needed to enhance competency and meet long-term mission requirements.

#### **Increasing Accountability**

To enhance mission performance and improve Departmental management, DHS must increase accountability across the organization. While accountability cuts across all aspects of the organization's operations, our initial focus will be to maximize the performance and resource data we collect to support strategic and risk-informed decision-making. The initiatives described below are intended to improve the effectiveness of the Department in turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan. DHS proposes to:

- Increase its analytic capability and capacity by enhancing strategic planning, resource allocation, risk analysis, net assessment, modeling capabilities, statistical analysis, and data collection;
- Improve performance measurement and accountability by increasing the quality of the Department's performance measures and linking those measures to the mission outcomes articulated in the QHSR Report; and
- Strengthen acquisition oversight by strengthening the Department's independent cost estimation capability.

## I. Introduction

The submission of the Quadrennial Homeland Security Review (QHSR) Report to Congress on February 1, 2010 marked an important first step in a multi-step process to examine and address fundamental issues that concern homeland security. The QHSR Report described the Nation's homeland security interests, identified the critical homeland security missions, and defined a strategic approach to those missions by laying out the principal goals, essential objectives, and key strategic outcomes necessary for that strategic approach to succeed.

**Figure 1. Homeland Security Missions and Goals**

<b>Mission 1: Preventing Terrorism and Enhancing Security</b>
<ul style="list-style-type: none"> <li>• Goal 1.1: Prevent Terrorist Attacks</li> <li>• Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities</li> <li>• Goal 1.3: Manage Risks to Critical Infrastructure, Key Leadership, and Events</li> </ul>
<b>Mission 2: Securing and Managing Our Borders</b>
<ul style="list-style-type: none"> <li>• Goal 2.1: Effectively Control U.S. Air, Land, and Sea Borders</li> <li>• Goal 2.2: Safeguard Lawful Trade and Travel</li> <li>• Goal 2.3: Disrupt and Dismantle Transnational Criminal Organizations</li> </ul>
<b>Mission 3: Enforcing and Administering Our Immigration Laws</b>
<ul style="list-style-type: none"> <li>• Goal 3.1: Strengthen and Effectively Administer the Immigration System</li> <li>• Goal 3.2: Prevent Unlawful Immigration</li> </ul>
<b>Mission 4: Safeguarding and Securing Cyberspace</b>
<ul style="list-style-type: none"> <li>• Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment</li> <li>• Goal 4.2: Promote Cybersecurity Knowledge and Innovation</li> </ul>
<b>Mission 5: Ensuring Resilience to Disasters</b>
<ul style="list-style-type: none"> <li>• Goal 5.1: Mitigate Hazards</li> <li>• Goal 5.2: Enhance Preparedness</li> <li>• Goal 5.3: Ensure Effective Emergency Response</li> <li>• Goal 5.4: Rapidly Recover</li> </ul>

This comprehensive, enterprise-wide strategic framework for homeland security provided the foundation for the next step: a deeper, bottom-up review of the Department of Homeland Security (DHS) programs and activities required to execute the homeland security missions. The bottom-up review (BUR) of DHS was initiated in November 2009 as an immediate follow-on and complement to the QHSR with the aim to align the Department's programmatic activities and organizational structure with the broader mission sets and goals identified in the QHSR.

This report is one result of that effort and represents an intermediate step between the QHSR Report and the DHS FY 2012 budget submission and corresponding FY 2012-2016 Future Years Homeland Security Program to Congress, which will propose specific programmatic adjustments based on the QHSR strategic framework. It provides the bridge between the homeland security

enterprise-level discussion in the QHSR Report and DHS responsibilities as they relate not only to the homeland security missions, but also to a number of other Departmental responsibilities as executed principally through several of its key operating components.

*Approach to the Bottom-Up Review*

The bottom-up review process gave DHS the opportunity to review its programmatic activities and organizational structure in depth. The aims were several-fold: first, to gauge how well current activities and departmental organization aligned with mission priorities and goals as outlined in the QHSR; second, to identify ways to achieve better programmatic and budgetary alignment across the entire department; third, to identify gaps in mission execution; and fourth, to prioritize initiatives to strengthen existing programs and organization, fill key gaps, and establish a foundation for innovation and advancement.

Three questions guided our work:

- How can we strengthen the Department's mission performance?
- How should we improve Departmental operations and management?
- How can we increase accountability for the resources entrusted to DHS?

DHS conducted extensive analysis of its current activities and organization in light of the mission goals and objectives set forth in the QHSR Report. The BUR Report describes DHS's current activities within each of the homeland security missions based on current authorities and roles and responsibilities, and sets forth DHS's conclusions concerning the priority initiatives and enhancements necessary to strengthen existing programs, fill shortfalls, and set a foundation for future success.

DHS used three criteria to evaluate mission, management, and accountability initiatives and identify enhancements:

- Does the initiative offer the opportunity to advance the safety, security, and resilience of the homeland beyond incremental improvements to current activities?
- Is the initiative sufficiently defined to permit the identification of performance objectives, measures, and targets?
- Can the initiative be achieved within the FY 2012-2016 timeframe?

In identifying initiatives across the homeland security mission space, three principal areas of emphasis became clear:

- Strengthen and Mature DHS—There is a need to strengthen the Department's ability to execute its mission responsibilities, run itself, and account for the resources that have been entrusted to it.



- Enhance Partner Capability and Capacity—Responsibilities for homeland security are broader than those of DHS and indeed broader than those of the Federal government. For that reason, there is a need to strengthen the ability of partners in the homeland security enterprise—in particular, State, local, tribal, and territorial governments, and the private sector—to execute important aspects of core homeland security mission activities.
- Deepen International Engagement—Finally, the security of our homeland begins far from our shores. We must work with key international partners to improve these critical partnerships and the activities that span the entire homeland security mission space, consistent with the broad range of U.S. Government international priorities and in consultation and coordination with the Department of State and the U.S. Chiefs of Mission in foreign countries.

The QHSR statute required an assessment of the organizational alignment of the Department with the national homeland security strategy and homeland security missions set forth in the QHSR Report. The BUR included this assessment. The BUR Report sets out initiatives and enhancements concerning DHS organization arising out of that assessment.

## **II. The Mission of the Department of Homeland Security**

The Department of Homeland Security was formed in the wake of the terrorist attacks of September 11, 2001 as part of a deliberate and determined national effort to safeguard the United States against terrorism. In March 2003, DHS became the third-largest Federal department, bringing together all or part of 22 different Federal agencies, each with a role in safeguarding the United States against terrorism.

From the outset, however, the Department's mission responsibilities went well beyond preventing terrorism, and included response to and recovery from natural disasters, customs enforcement and collection of customs revenue, administration of legal immigration services, safety and stewardship of the Nation's waterways and marine transportation system, as well as other legacy missions of the various components of DHS. This breadth of mission responsibilities reflects the richness, history, and diversity of DHS components and the need to safeguard this country from a variety of threats and hazards.

In addition to combining 22 separate pre-existing entities, the creation of DHS included the establishment of a headquarters that includes management, science and technology, intelligence and analysis, policy, operations, and legal functions, specialty expertise in health affairs, domestic nuclear detection, and counternarcotics enforcement coordination, a citizenship and immigration services ombudsman, and the Federal Law Enforcement Training Center. DHS also placed a strong emphasis on cybersecurity and infrastructure protection within the National Protection and Programs Directorate. Annex A describes the main elements of the DHS force structure within the seven DHS operational components.

DHS headquarters also includes several offices with critical responsibilities for internal DHS coordination as well as communication and connection with the Department's external

stakeholders, including public affairs, legislative affairs, intergovernmental affairs, State and local law enforcement, and the private sector, as well as offices focused on privacy, civil rights, and civil liberties. At DHS, clear and consistent communication with the general public, State, local, tribal, and territorial governments, as well as Congress is critical to advancing our priorities across a diverse and complex mission space from counterterrorism and countering violent extremism to individual, family, and community preparedness and resilience. Equally important, these offices ensure the Department's commitment to the preservation of privacy, civil rights, and civil liberties with respect to homeland security activities.

The mission of DHS is carried out through the tireless and dedicated efforts of more than 200,000 men and women who serve at the Department. As we act to strengthen and mature DHS and enhance our capability, DHS will ensure that its workforce is engaged in our mission, resilient, and properly trained. DHS will also continue to foster an environment where our employees understand the critical importance of their work and how their efforts contribute to the Department's goals. Annex B sets forth the range of DHS activities on any given day.

Integrating the many disparate entities of DHS—some with long histories of independent or autonomous operations, and all with distinct operational cultures—while maintaining their unique strengths and capabilities has presented significant public policy and management challenges. DHS recognizes the difficulty of this task, and through the QHSR and BUR processes has sought to deliberately and incrementally move DHS towards a more unified and integrated posture.

### **III. Enhancing Mission Performance**

#### **A. Preventing Terrorism and Enhancing Security**

##### *Current Authorities*

Under the Homeland Security Act of 2002, the primary mission of the Department of Homeland Security begins with preventing terrorist attacks within the United States and reducing the vulnerability of the United States to terrorism. The Homeland Security Act specifies that the Secretary of Homeland Security is responsible for preventing the entry of terrorists and the instruments of terrorism into the United States. The act requires the Secretary to access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in order to identify and assess the nature and scope of terrorist threats to the homeland; detect and identify threats of terrorism against the United States; and understand such threats in light of actual and potential vulnerabilities of the homeland.

The Homeland Security Act also makes the Secretary of Homeland Security responsible for coordinating overall efforts to manage risk to critical infrastructure and key resources; Homeland Security Presidential Directive 7 reinforces and describes this authority. The Secretary of Homeland Security is also vested with a range of authorities relating to chemical, biological, radiological, and nuclear (CBRN) countermeasures, biosurveillance, domestic nuclear detection,

transportation of hazardous materials, chemical facility security, as well as broad customs authorities to prevent the importation of dangerous materials, including CBRN weapons and materials. The Aviation and Transportation Security Act of 2001, the Maritime Transportation Security Act of 2002, the Intelligence Reform and Terrorism Protection Act of 2004, and the SAFE Port Act of 2006 authorize a range of aviation, maritime, and surface transportation system security activities aimed at the deterrence, detection, and disruption of terrorist activities against the transportation sector, and Title 18 of the United States Code vests the Department, through the U.S. Secret Service, with responsibilities for protecting the President, the Vice President, national leaders, foreign heads of state and government, as well as certain facilities and events.

#### *Overview of the DHS Role*

Protecting the United States and its people from terrorism is the cornerstone of homeland security. This mission includes three goals:

- (1) Preventing terrorist attacks;
- (2) Preventing the unauthorized acquisition or use of CBRN materials and capabilities within the United States; and
- (3) Reducing the vulnerability of critical infrastructure to terrorist attacks and other hazards.

DHS shares the responsibility to prevent terrorist attacks with several Federal departments and agencies. The Departments of State, Justice, and Defense, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) all have leadership roles and responsibilities in the U.S. government's efforts to prevent terrorist attacks. For example, the NCTC maintains the Terrorist Identities Datamart Environment (TIDE). The FBI administers the Terrorist Screening Center, which determines which individuals will be placed into the Terrorist Screening Database—the comprehensive terrorist watchlist—and administers the process by which the No Fly and Selectee lists are derived. The FBI and the Department of Justice also lead terrorism investigations; coordinate law enforcement efforts to detect, prevent, and disrupt terrorist attacks against the United States; and are responsible for the related intelligence collection activities within the United States. DHS operates as a principal consumer of NCTC and FBI watchlist products for DHS border and aviation security operations and vetting of key transportation workers. Also, DHS is a partner in data sharing and threat analysis, and supports the NCTC and national network of the FBI Joint Terrorism Task Forces. DHS intelligence entities—including intelligence elements within several DHS operational components—gather, share, and disseminate intelligence between the field and the larger Intelligence Community.

In support of several recent, high-profile counterterrorism investigations, DHS institutionalized an integrated DHS Threat Task Force (DTTF), composed of staff from multiple operational components of the Department who work alongside analysts from the Office of Intelligence and Analysis. The DTTF directly supports FBI investigations, ensures coordination across DHS, expedites cross-checking of Departmental data holdings for the National Targeting Center and other purposes, and provides time-urgent threat information to DHS leadership and, in coordination with the FBI, frontline law enforcement.

### Preventing Terrorist Attacks

Within the context of coordination and collaboration with State, local, tribal, and territorial governments, nongovernmental organizations, and the private sector, the Department is charged with assisting State, local and private sector entities in disrupting potential terrorist activity and denying terrorists access to the United States at our land, air and sea ports of entry, as well as travel networks into and within the country.

DHS has adopted a multi-faceted approach to enhance aviation security capabilities both at home and abroad. DHS has the lead in three areas: (1) pursuing enhanced screening technology, protocols, and procedures, especially regarding aviation and other transportation sectors, consistent with privacy rights, civil rights, and civil liberties; (2) strengthening international partnerships and coordination on aviation security issues; and (3) developing recommendations on long-term law enforcement requirements for aviation security in coordination with the Department of Justice. In addition, DHS supports the Intelligence Community's efforts to re-evaluate and modify the criteria and processes used to create watchlists.

DHS devotes significant frontline resources to preventing terrorists from traveling to and within the United States and seizing prohibited materials that they may use in an attack. Through such activities as terrorist watchlists and targeting systems for vetting of passengers, physical screening of passengers and crew, baggage, and cargo, patrol and surveillance of our nation's borders, and counter proliferation and financial crimes investigations and substantial support to the FBI Joint Terrorism Task Forces, DHS attempts to deter, detect, mitigate, and prevent terrorist attacks on the homeland. TSA is working to improve security in the surface modes of transportation by performing risk assessments, closing vulnerability gaps, vetting key workers, providing training, conducting exercises, and deploying Visible Intermodal Prevention and Response teams (VIPRs).

DHS responsibilities for preventing terrorist attacks include assisting State, local, tribal, and territorial governments to obtain the information and capabilities to address threats. To this end, DHS awards almost \$4 billion annually to State, local, tribal, and territorial governments through the State Homeland Security Grant Program, the Urban Areas Security Initiative, and other grant programs. These grant programs help State, local, tribal, and territorial governments build and sustain capabilities necessary to prevent terrorist attacks, as well as address other threats, prepare for, respond to, and recover from all hazards, and build additional public safety capability.

One prime example of these State, local, tribal, and territorial capabilities are fusion centers, which receive pertinent threat and risk information and analysis from the Intelligence Community and other Federal entities while also helping States and major municipalities collect, aggregate, fuse, and disseminate homeland security-related intelligence, law enforcement, and risk information to frontline officers and first responders, as well as back to the Intelligence Community and other Federal partners. In close partnership with this network of fusion centers, DHS plays a key role in preventing terrorist attacks that originate from within the United States.

#### Preventing the Unauthorized Acquisition or Use of CBRN Materials and Capabilities

While a variety of Federal departments and agencies are responsible for preventing the unauthorized acquisition or use of CBRN materials and capabilities, DHS plays a critical role in integrating these activities through programs implemented by U.S. Customs and Border Protection (CBP), the U.S. Coast Guard (USCG), the Domestic Nuclear Detection Office (DNDO), the Science and Technology Directorate (S&T), and other Departmental elements. DHS secures global trade and travel systems, investigates criminal activities involving the unlawful import and export of CBRN materials, technologies and capabilities, and detects and counters the importation and movement of CBRN weapons and materials into or already within the United States. In particular, the threat of nuclear terrorism is fundamentally unlike any of the other threats that DHS must prevent. The potential consequences of an attack using an improvised nuclear device require that the Department maintain a continued focus on prevention.

DHS prevents weapons of mass destruction and weapons of mass effect from entering the United States at and between ports of entry, investigates violations relating to the importation of CBRN materials, and regulates the security of high-risk chemical facilities. DHS has a specific focus on coordinating Federal efforts to detect and protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States. In addition, through the BioWatch program, which deploys sensor technology to detect the presence of biological agents, DHS coordinates with Federal, State, local, tribal, and territorial partners for management of biological attacks. DHS also provides substantial financial support and technical assistance to State, local, tribal, and territorial governments through grant programs for CBRN detection.

#### Managing Risks to Critical Infrastructure, Key Leadership, and Events

DHS has national leadership responsibilities for managing risks to critical infrastructure, key resources, and events. The Secretary of Homeland Security is vested by statute and Presidential directive with coordinating national efforts to secure and protect critical infrastructure and key resources, which the Department does currently through the National Protection and Programs Directorate (NPPD). Through communication and coordination with governmental and private sector partners, DHS leads the national effort to mitigate terrorism risk to, strengthen the protection of, and enhance the all-hazard resilience of the Nation's critical infrastructure across the identified 18 sectors. DHS is also the Sector-Specific Agency for 11 of the 18 critical infrastructure sectors set forth in the *National Infrastructure Protection Plan*: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Emergency Services, Government Facilities, Information Technology, Nuclear Reactors, Materials and Waste, Postal and Shipping, and Transportation Systems. The U.S. Secret Service (USSS) has critical responsibilities for criminal investigations relating to the integrity of the financial system and the counterfeiting of U.S. currency. In addition, U.S. Immigration and Customs Enforcement (ICE) targets the underlying cross-border financial systems that terrorist and transnational criminal organizations may exploit in raising, moving, and storing illicit funds. ICE also seeks to deny transnational criminal organizations access to these systems. Annex E sets forth the 18 critical infrastructure sectors and the Sector-Specific Agency for each.

Through the Secret Service, DHS also has the unique responsibility to protect the President, the Vice President, visiting heads of state, and major Presidential candidates, as well as to ensure the continuity of national leadership. Protection includes all activities related to identifying threats, mitigating vulnerabilities, and creating secure environments wherever protectees work, reside, and travel. The Secret Service also coordinates protective intelligence investigations through its network of field offices and leads the design and implementation of operational security plans and protective activity for National Special Security Events. The Secret Service also has critical responsibilities for criminal investigations relating to the integrity of the financial systems and counterfeiting of United States currency.

#### *Initiatives and Enhancements*

The QHSR and BUR analyses suggest several priority initiatives, as well as enhancements to current programs, in order to better prevent terrorism and enhance security. Innovations like the DTF represent a major step forward in coordinating counterterrorism activities, but DHS must find ways to further centralize coordination to leverage operational, intelligence, and strategic synergies across the department. Similarly, DHS must better leverage the critical information it receives across a wide range of mission-based and functional activities, while protecting privacy, civil rights, and civil liberties. Recent aviation security successes have laid the groundwork for further and necessary improvements in technology, process, and partnerships, and these efforts must remain an urgent mission priority. As threats evolve and complexity increases across the homeland security enterprise, standardization has become critically important. While our partnerships for critical infrastructure protection remain strong and continue to grow, we must strive to more effectively push information and knowledge out to the field where it is most urgently needed.

To address these challenges, the Department will strengthen counterterrorism coordination across DHS, strengthen land, maritime, and aviation security both domestically and abroad, create an integrated Departmental information sharing architecture, deliver infrastructure protection and resilience capabilities to the field, set national performance standards for identity verification, and increase efforts to detect and counter nuclear and biological weapons and dangerous materials. We will also enhance partner capability and capacity—particularly at the State, local, tribal, and territorial level—by standardizing and institutionalizing the National Fusion Center Network, pursue initiatives to safeguard access to secure areas in critical facilities, make DHS a center of excellence for canine training and deployment, and redesign the Federal Protective Service (FPS) to become a model critical infrastructure protection and law enforcement agency for the government sector and better match mission requirements.

- *Strengthen counterterrorism coordination across DHS.* Although DHS is one of the Federal government's key counterterrorism agencies, beyond the Secretary and Deputy Secretary, DHS did not have a single coordinating entity for counterterrorism activities. DHS recently designated a Coordinator for Counterterrorism who is responsible for coordinating all counterterrorism activities for the Department and across its directorates, components, and offices. DHS will continue to evolve the Counterterrorism coordination function in consultation with Congress.

- *Strengthen aviation security.* The attempted terrorist attack on Flight 253 on December 25, 2009, illustrates the continuing and evolving nature of the threat to the aviation transportation system. DHS has lead responsibilities for aviation security and is also embarking on a major global initiative to improve aviation security technology and processes around the world. DHS is also partnering with the Department of Energy—including the National Laboratories—and private industry to develop new and more effective technologies to deter and disrupt known threats and proactively anticipate and protect against new ways by which terrorists could seek to board an aircraft. DHS will also collaborate with the aviation industry to use a risk-based approach to inform decisions about changes to operations, business processes, and aircraft development. In all cases, DHS will use current intelligence-derived threat information to drive day-to-day operations. DHS will also work with other Federal, State, local, tribal, and territorial law enforcement partners and airport authorities to implement long-term, sustainable aviation security law enforcement. State, local, tribal, and territorial law enforcement and airport authorities play a critical role in our aviation security success.
- *Create an integrated Departmental information sharing architecture.* Given its daily interaction with the global movement of people and goods, DHS is uniquely authorized and positioned to fuse and analyze intelligence, law enforcement, screening, and other information gathered through encounters with travelers and commercial entities in order to prevent terrorist travel, finance, and operations. While the establishment of the DHS Threat Task Force was a step forward in data sharing, more work can be done to enhance DHS' ability to access information in near-real time and use it to identify people and goods posing high risk to the United States while protecting privacy, civil rights, and civil liberties. In order to accomplish this goal, DHS will create an information sharing architecture to consolidate and streamline access to intelligence, law enforcement, screening, and other information across the Department. That architecture will include the capability for automated recurrent screening and vetting for individuals to whom DHS has provided a license, privilege, or status (including immigration status) so that, as new information becomes available, DHS can assess whether the individual is no longer eligible for the benefit or presents a threat. It will also include the capability to conduct scenario-based automated targeting of individuals and other entities using intelligence-driven criteria.
- *Deliver infrastructure protection and resilience capabilities to the field.* Develop, deliver and continuously update a portfolio of DHS and Federal agency-wide capabilities, tools and products (e.g. from our partners in the Sector Specific Agencies) for critical infrastructure protection and resilience to State, local, tribal and territorial government and their local and regional partners and the private sector, tailored and supported based on regional and local needs. DHS will conduct these activities as it explores opportunities with the private sector to "design-in" greater resilience for critical infrastructure as described in "Ensuring Resilience to Disasters," below.
- *Set national performance standards for identification verification.* In order to meet the 9/11 Commission's recommendation regarding the security of State drivers' licenses and identification cards, DHS has supported the efforts of Governors and Congress to enact

the *Providing for Additional Security in States' Identification Act* (PASS ID). PASS ID puts States on the path to implementing national standards for identification documents and will strengthen security across the country while enhancing privacy safeguards and protection of personally identifiable information. Although the May 2011 deadline for full compliance with the REAL ID Act remains in effect, legislative action is needed to address systemic problems with REAL ID to advance our security interests over the long term. DHS is committed to moving forward both administratively and with Congress to implement this key 9/11 Commission recommendation to help prevent terrorism, reduce fraud, and improve the reliability and accuracy of personal identification documents.

- *Increase efforts to detect and counter nuclear and biological weapons and dangerous materials.* DHS will prioritize nuclear detection research and development and also work with the Intelligence Community to develop intelligence and analysis capabilities relating to improvised nuclear devices and radiological dispersal devices, to include developing the capability to detect and react to pre-detonation cues or signatures to provide early-warning indicators of an imminent or credible threat of a terrorist attack using a nuclear weapon. DHS, working with its partners in the interagency, will also use the most advanced tools to facilitate investigations against vendors, buyers, and traders who violate export control laws and unlawfully transfer nuclear and biological technology over the Internet or controlled material of select agents anywhere. In addition, DHS will place greater emphasis on biological detection and countermeasures and accelerate development of forensics capabilities for biological weapons in order to help attribute those attacks to a particular country or group. These efforts will include increasing the capabilities of the DHS National Biodefense Analysis and Countermeasures Center (NBACC), which carries out many of these activities. DHS will also look to increase its international capabilities to track the evolution and migration of potentially high-consequence human, animal, and plant diseases.
- *Leverage the full range of capabilities to address biological and nuclear threats.* As noted above, in addition to increasing efforts to detect and counter nuclear and biological weapons and dangerous materials, DHS will increase its leadership role in protecting against biological and nuclear threats more generally. The DHS Office of Health Affairs (OHA) and the Domestic Nuclear Detection Office (DNDO) each bring critical capabilities to this effort. OHA concentrates mainly on chemical and biological threats and their consequences. DNDO focuses on detecting the presence of nuclear weapons and materials through implementation of the Global Nuclear Detection Architecture and assistance with attribution of interdicted nuclear material through the National Technical Nuclear Forensics Center. DHS will leverage these capabilities, while enhancing coordination with Federal, State, local, tribal, territorial, nongovernmental, and private sector partners on CBRN issues.
- *Standardize and institutionalize the National Fusion Center Network.* Since 2003, a national network of fusion centers has developed at the State, local, tribal, and territorial level, supported by funding, training, exercises, and technical assistance from DHS and the Department of Justice. However, to date, there has been no systematic effort to ensure that these centers establish and maintain a baseline level of capability so that they



are able to become fully integrated into national efforts to gather, analyze, and share information needed to protect our communities. DHS has proposed a new National Fusion Center Program Management Office to assess the current level of capability of fusion centers and to support their meeting defined outcomes, national standards, and baseline levels of capability with Federal, State, local, tribal, and territorial partners, and the private sector.

- *Promote safeguards for access to secure areas in critical facilities.* Employees or other trusted or credentialed individuals who harbor malicious intentions present a pernicious challenge to safeguarding access to secure areas in critical facilities such as airports. To protect against this threat, DHS will expand risk-informed screening and recurrent vetting in the transportation sector to include additional populations of aviation and surface transportation workers in order to validate both the identity and the integrity of individuals with access to critical or sensitive infrastructure. DHS will also implement processes to recurrently vet all Federal employees, contractors, and Federal secure identification credential holders.
- *Establish DHS as a center of excellence for canine training and deployment.* Canines serve essential roles in homeland security. Specially-trained canines and their handlers are essential elements of terrorism prevention efforts at the Federal, State, local, tribal, and territorial levels and in the private sector. Canines also serve essential roles in detecting narcotics at the air, sea, and land ports of entry, and in search and rescue activities following disasters. DHS will increase specialized breeding activities for canines, enhance its training and certification of canines and handlers, and become a center of excellence for employment of canines across the homeland security missions.
- *Redesign the Federal Protective Service (FPS) to better match mission requirements.* FPS is responsible for protecting most facilities occupied or secured by the Federal government and the people in those facilities through the application of law enforcement and physical security authorities. (FPS is not responsible for certain Federal facilities, including military facilities such as the Pentagon.) In 2009, DHS transferred responsibility for FPS from ICE to NPPD. DHS now proposes to undertake a major redesign of FPS, in coordination with the U.S. General Services Administration, to set the future vision for FPS and define roles and responsibilities consistent with the fulfillment of this vision. The FPS redesign will create functional alignment within FPS and between FPS and other elements of DHS, better match mission requirements to the risk profiles of both leased and owned public buildings and infrastructure nationwide, and set FPS on a course to become a model critical infrastructure protection and law enforcement agency. Such an effort entails the realignment of the workforce to better match mission needs and customer expectations. Inherent in this effort is the need for a more capable Federal workforce, exploration of additional authorities, an increased use of innovative security technologies, and an examination of the optimal funding mechanism for securing and protecting facilities occupied by the Federal government.

## **B. Securing and Managing Our Borders**

### *Current Authorities*

Under the Homeland Security Act, the Secretary of Homeland Security is responsible for securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems of the United States. This authority includes administration of the customs laws of the United States, and responsibility for ensuring the speedy, orderly, and efficient flow of people, goods, and information. The DHS is also responsible for monitoring connections between illegal drug trafficking and terrorism, coordinating efforts to sever such connections, and otherwise contributing to efforts to interdict illegal drug trafficking and its ill-gotten proceeds. The Immigration and Nationality Act of 1952, as amended, provides authority for the enforcement of the immigration laws to include immigration inspections and human smuggling interdiction at ports of entry as well as for the U.S. Border Patrol, part of CBP. Titles 14 and 19 of the United States Code provides broad customs enforcement authorities for securing and managing the movement of merchandise, people, conveyances, containers, and mail into and out of the United States, and the Tariff Act of 1930, as amended, provides that Customs officers enforce all laws relating to the assessment and collection of customs duties and related responsibilities. The Ports and Waterways Safety Act of 1972 and the SAFE Port Act of 2006 provide authorities for securing seaports and the international supply chain, as well as broad authority for the interrelated functions of promoting vessel safety and the protection of the marine environment; the Aviation and Transportation Security Act of 2001 provides authorities to protect the air transportation system. Homeland Security Presidential Directive 11 vests the Secretary of Homeland Security with leadership responsibilities for coordinating screening of people and cargo, and Homeland Security Presidential Directives 13 and 16 vest the Secretary of Homeland Security with leadership responsibilities for maritime and aviation security, respectively.

### *Overview of the DHS Role*

We are responsible for secure, well-managed borders that not only protect the United States against threats from abroad, but also expedite the safe flow of lawful travel and commerce. Achieving this outcome depends on achieving three interrelated goals: (1) effectively securing U.S. air, land, and sea borders; (2) safeguarding lawful trade and travel; and (3) disrupting and dismantling transnational criminal organizations.

Working with our partners both nationally and internationally, our strategy is to manage and secure our Nation's borders by employing and enhancing our layers of security through the continuum that impacts our borders—starting from the point of origin overseas where people and cargo originate, through transit to the United States, the arrival and entry at our borders, then on to the routes of egress away from the border and ultimately to the final destination within the United States. This strategy relies upon using increased intelligence and risk management strategies in order to segment, sort, target, triage, and expedite the movement and flow of travelers and trade. We must constantly reevaluate and improve our effectiveness along each step of this continuum to ensure that we continue to be proactive in our approach to the security of our Nation.

### Effectively Securing U.S. Air, Land, and Sea Borders

The border environment is characterized by three different areas of activity: (1) ports of entry, such as airports, seaports, and land border crossings; (2) areas between ports of entry; and (3) the approaches to our borders—the areas leading up to and surrounding U.S. borders. The border environment also includes those areas over which DHS components assert, exercise, and enforce legal jurisdiction (e.g. U.S. Territorial Sea, Contiguous Zone, Exclusive Economic Zone, and on U.S. vessels on the high seas). DHS relies on a combination of people, technology, and infrastructure (e.g. roads, fences) across DHS operating components to secure the border.

Through CBP and the U.S. Coast Guard (USCG), DHS is responsible for securing and enforcing U.S. law at the Nation's international borders, as well as at the over 300 official Ports of Entry, international mail facilities, and other points of entry to the United States. Along these borders and at these entry points, DHS is the key interface for America's international trading partners, for travelers seeking to enter or leave the United States, and for businesses seeking to import or export goods into or out of the United States. DHS also defends against transnational criminal or terrorist organizations seeking to exploit vulnerabilities in our open society, smuggle dangerous people, weapons, or goods into or out of our country, or attack critical border infrastructure.

At ports of entry in the air domain (airports with international flight arrivals), land domain (land border crossings), and maritime domain (seaports), DHS is responsible for physically screening people and goods upon their arrival to the country. DHS's work begins well before people and goods arrive at our borders. Using a variety of intelligence, automated tools, and information collected in advance of arrival for passengers and cargo, DHS works to screen, identify, and intercept threats at points of departure before they reach our shores. DHS conducts these activities in conjunction with international partners and the private sector through CBP-led programs such as the Container Security Initiative and Immigration Advisory Program. Similarly, through USCG, the Department ensures vessel security and compliance with both domestic and international safety and security standards through imposing Conditions of Entry on vessels and enforcing 96-hour Advance Notice of Arrival requirements. These programs ensure the security and resilience of the key global systems and networks essential to the U.S. and global economies.

Between ports of entry—where in the land domain all flows are by definition illegal—agents, technology, and infrastructure combined with a defense in-depth enforcement strategy are all key components of effective border security. DHS uses air, land, and marine assets to patrol and secure U.S. borders, as well as sophisticated systems to effectively detect and interdict potential threats beyond our borders. USCG provides air and maritime patrols along the U.S. border, including seacoasts, lakes, and rivers, where USCG and CBP have explicit legal authorities to enforce a broad array of U.S. laws designed to safeguard, secure, and protect U.S. citizens, vessels, and resources. In the approaches to the United States, CBP and USCG both maintain domain awareness efforts to establish and maintain situational awareness and a common operating picture of people, vehicles, aircraft, and marine vessels approaching our borders. Additionally, larger, more capable USCG afloat and air assets maintain an offshore presence to actively monitor offshore activity and engage when necessary to execute a layered approach to

securing our maritime borders. DHS works closely with other Federal departments and agencies, such as the Departments of Justice, Transportation, and Defense, in conducting these activities. Effective, real-time coordination of interagency activities is critical for success in this cross-domain environment.

#### Safeguarding Lawful Travel and Trade

DHS plays an essential role in safeguarding lawful travel and trade. To do so most effectively, we must seek ways to interdict threats at the earliest point through international partnerships, better use of technology, and increased intelligence. Equally critical to ensuring the health of our economy is the need to enable the secure, lawful flow of people and goods into and out of the United States. DHS efforts entail both foreign and domestic activities and focus on the global trade and travel system and the risk posed by people and goods in transit.

Through the Transportation Security Administration (TSA), USCG, ICE, and CBP, DHS is active in global standard-setting organizations—such as the International Civil Aviation Organization, the International Maritime Organization, and the World Customs Organization—to create global standards for security and resilience of global trade and travel systems. In addition, TSA conducts inspections of foreign airports with direct flights to the United States in order to ensure adherence to international and TSA aviation security standards. Domestically, TSA regulates security of airports, including those with international arrivals, and CBP and USCG secure seaports and land ports of entry. USCG works closely with foreign navies and coast guards to enhance the inherent maritime port security capabilities of trading partners, in addition to regularly visiting foreign ports to ensure port facility security measures meet international standards.

CBP works with international customs and border agencies, as well as the trade community (including shippers, importers, brokers, and bonding companies), to ensure the security and integrity of foreign transactions and exchanges along global supply chains. This includes facilitating the flow of legitimate trade across U.S. borders while securing our borders and helping to protect the American economy from illicit commercial enterprises. This includes helping to protect American businesses from theft of intellectual property and unfair trade practices, enforcing trade laws related to admissibility, and protecting the American public from health and public safety threats.

DHS components work to secure modes of transportation and their crews. TSA works with domestic and foreign airlines, as well as aircraft manufacturers, to ensure the integrity of aircraft and air crews, and works with the air cargo supply chain to ensure the integrity of cargo transported on passenger aircraft. USCG regulates vessel owners and operators and conducts regular inspections for safety and security purposes. CBP works with shippers to ensure the integrity of international shipments and cargo containers and vets crew members of vessels and passenger ships.

DHS also plays an important role in managing the risk of people and goods in transit to the United States. DHS maintains databases of information consistent with privacy, civil rights, and civil liberties safeguards, enforcing security standards for travel documents, and detecting the use

of fraudulent documents in order to identify terrorists, criminals, and other risks. Through the Secure Flight program, DHS will ensure consistency in the vetting of domestic and international passengers against terrorist databases. Through resources such as the National Targeting Center, DHS screens people, goods, and conveyances bound for the United States through air, land, and sea routes, and provides information to agents and officials on the ground to intercept known and suspected threats. DHS also posts officers to foreign ports and works collaboratively with foreign countries, port operators, and shipping companies to screen cargo, investigate visa applications, and collaborate on aviation security. While the Department of State adjudicates and issues visas abroad, DHS—primarily through its visa security units—works closely with the Department of State in many countries where applicants present the highest threat in order to reduce the risk of terrorist or transnational criminals receiving a visa.

Through an automated risk assessment process, CBP screens 100 percent of all arriving cargo using advanced manifest data. Shipments posing a potential risk are identified prior to departure for maritime cargo, and prior to arrival into the U.S. port of entry for air and land cargo. Maritime cargo identified as high risk may be examined overseas, as part of the Container Security Initiative, which is in operation at 58 seaports worldwide, representing over 80 percent of the maritime cargo destined for the U.S. worldwide. At U.S. ports of entry, CBP uses radiation portal monitors to scan arriving cargo for radiation. Currently, 100 percent of the cargo and vehicle traffic at our land ports of entry and 99.3 percent of containerized maritime cargo at our seaports are scanned. TSA will implement 100 percent screening of air cargo on passenger aircraft traveling point-to-point domestically and departing from the U.S. for foreign destinations by August 2010, and is working with the international air cargo community to increase screening of air cargo on inbound international passenger aircraft.

As an interrelated function with respect to lawful trade, the Department, through CBP, also proactively facilitates trade and collects over \$34 billion in customs revenue each year for the United States treasury.

#### Disrupting and Dismantling Transnational Criminal and Terrorist Organizations

DHS is the Federal government's largest law enforcement department. CBP and ICE have broad investigatory and enforcement authorities that cover not only immigration violations but also a wide range of border-related crime, including violations of U.S. customs, import, and export control laws. ICE investigates violations of over 400 statutes that protect the U.S. against the unlawful entry and export of people, goods, and monetary instruments. ICE works closely with other DHS law enforcement agencies, such as CBP, TSA, and USSS, as well as with other Federal law enforcement agencies, such as the FBI, the Drug Enforcement Administration, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and the U.S. Postal Inspection Service to investigate transnational criminal organizations that engage in smuggling and trafficking across the U.S. border. Human smuggling and trafficking, child sex tourism, counter proliferation, financial, intellectual property, weapons trafficking, and narcotics investigations are among ICE's top investigative priorities. DHS conducts investigations through its Border Enforcement Security Taskforces (BESTs) and Integrated Border Enforcement Teams (IBETs) that combine CBP and ICE agents and officers with Federal, State, local, tribal, and territorial law enforcement partners, as well as international partners, to interdict illegal drug trafficking, detect and disrupt

illicit pathways used by transnational criminal and terrorist organizations, and arrest foreign nationals attempting to enter the United States illegally.

#### *Initiatives and Enhancements*

The QHSR and BUR analyses presented several opportunities for improvement. While effective mechanisms exist for interagency and intra-Departmental operational and intelligence coordination, we must learn from the successes of Joint Interagency Task Force-South (JIATF-South) and other similar constructs to further integrate and enhance domain awareness across our efforts to secure the border and expedite lawful travel and trade. Our investigations portfolio focused on transnational criminal and terrorist organizations must reflect our priorities and adopt a more proactive posture. We must do more to directly support key international partners in their efforts, both with respect to training and technical assistance, and direct coordination, information sharing, and joint risk assessments.

Therefore, in order to strengthen efforts to secure and manage our borders, the Department will seek to expand joint operations and intelligence capabilities, including enhanced domain awareness, prioritize immigration and customs investigations on the security of global trade and travel systems, enhance the security of global trade and travel systems, expand DHS international border integrity and customs enforcement security assistance, and work closely with the governments of Canada and Mexico to enhance North American security.

- *Expand joint operations and intelligence capabilities, including enhanced domain awareness.* DHS will unify the uses of technology, surveillance capabilities, and related resources across air, land, and maritime domains, with an increased emphasis on data collection, data processing, and integrating sensors across domains. DHS will harmonize operations and intelligence—utilizing concepts and structures modeled after JIATF-South, as appropriate—for the geographical approaches not covered by JIATF-South, such as the southwest border, as well as for arrivals of people and goods into the United States. Working with its partners, including the Department of Justice and the Office of National Drug Control Policy, DHS also will build upon the successful models established as part of our interagency counternarcotics infrastructure—including the Air and Marine Operations Center, the El Paso Intelligence Center, and other DHS and U.S. government operations centers—to apply those models more broadly to the spectrum of homeland security challenges across the air, land, and maritime domains. Finally, DHS will establish and coordinate cross-domain operational threat analysis and response protocols in order to ensure greater effectiveness of interagency and intergovernmental response to threats across air, land, and maritime domains.
- *Prioritize immigration and customs investigations on the security of global trade and travel systems.* DHS law enforcement agencies have substantial authorities to disrupt and dismantle transnational criminal and terrorist organizations that seek to exploit lawful trade and travel systems and establish illicit pathways for the movement of people and goods. DHS will strategically prioritize investigations to focus proactively on security of the global trade and travel system that directly affect immigration and customs activity across U.S. borders. Priorities within this proactive investigative portfolio will include

human smuggling and trafficking, child sex tourism, counter proliferation, financial, intellectual property, weapons trafficking, and narcotics investigations.

- *Enhance the security and resilience of global trade and travel systems.* As described in the QHSR Report, securing and managing our borders is about more than the physical border environment. We must enable the secure, lawful flow of people and goods into and out of the United States. To that end, DHS will continue the development and implementation of trusted traveler and trusted shipper programs in order to increase our knowledge of people and goods that pose low risk traveling or transiting in global trade and travel systems. DHS will also enhance the sophistication of its information sharing architecture in order to evaluate the risk posed by people and goods in transit while safeguarding privacy, civil rights, and civil liberties. Trusted traveler and shipper programs and a more sophisticated information sharing architecture will allow DHS and its partners to focus information collection, targeting, and interdiction efforts on people and goods known or believed to pose high risk to the United States. To support these efforts, we will strengthen international information sharing agreements regarding criminals, terrorists, and individuals with suspected ties to terrorists and collaborate with the Department of State to institutionalize enhanced visa security programs at high-risk visa adjudication posts.
- *Strengthen and expand DHS-related security assistance internationally (e.g. border integrity and customs enforcement security assistance) consistent with U.S. government security, trade promotion, international travel, and foreign assistance objectives.* Our national security depends on the ability of foreign governments to effectively combat terrorism and other threats within their own borders. DHS has substantial capability and capacity to help implement assistance and training to foreign governments in areas such as biometrics, document fraud, aviation security, port and maritime security, cargo security, bulk cash smuggling, customs enforcement, and human smuggling and trafficking. The U.S. government, through the Departments of State and Defense, provides security assistance and foreign assistance to legitimate members and representatives of foreign security forces and civilian institutions. This includes providing resources to institutions related to homeland security in foreign countries—including land and maritime border integrity and customs enforcement functions. DHS believes that training and technical assistance for international security partners in the areas of border integrity and customs enforcement must be increased. DHS also supports the strengthening of security to facilitate travel and commerce for legitimate travelers and goods. DHS will work in consultation and coordination with the Departments of State and Defense, as well as with Congress, to ensure adequate resources to support these purposes. DHS will also coordinate a proposal with the Department of Defense (DOD) to post DHS liaison officers in each of the DOD geographic commands to coordinate and integrate homeland security-related assistance funding aims. Finally, DHS will explore the expansion of additional international partnerships for homeland security-related activities as appropriate, in consultation and coordination with the Department of State and, where appropriate, DOD, including current activities such as visa security and international law enforcement training.

- *Enhance North American security.* Our efforts to secure and manage our borders will be most effective when we work collectively with our North American partners, Canada and Mexico. To that end, DHS will enhance information sharing with Federal, State, local, tribal, nongovernmental, private sector, and international partners along the Northern and Southern borders. DHS will also foster cross-border threat and risk assessments and enhanced coordination and cooperation on securing the transnational flow of people and goods through expanding joint efforts and shared resources.

Our efforts to strengthen DHS intelligence and information sharing capabilities described above in the “Preventing Terrorism and Enhancing Security” section will also assist these efforts.

### **C. Enforcing and Administering Our Immigration Laws**

#### *Current Authorities*

Pursuant to the Homeland Security Act, the Secretary of Homeland Security is responsible for establishing national immigration enforcement policies and priorities and administering the lawful immigration system, including establishing and administering rules governing the granting of visas, refugee, and asylum or other forms of permission to enter the United States. The Immigration and Nationality Act of 1952, as amended (INA), provides the Secretary with authority to administer the immigration laws of the United States as well as authority to arrest, detain, prosecute, and remove unauthorized foreign nationals present in the United States, especially those identified as criminals, fugitives, and otherwise dangerous. The INA confers authority to investigate civil and criminal violations of immigration laws, including human smuggling and fraud investigations.

#### *Overview of the DHS Role*

Smart and effective enforcement and administration of U.S. immigration laws allows the government to facilitate lawful immigration while identifying and removing those who violate our laws. Enforcing and administering our immigration laws depends on (1) strengthening and effectively administering our immigration system; and (2) preventing unlawful immigration.

#### Strengthening and Effectively Administering the Immigration Services System

As noted above, the Homeland Security Act of 2002 vests the Secretary of Homeland Security with the authority to set immigration and visa policy and administer the immigration system, with the INA serving as the basic immigration law of the United States. DHS works with other Federal departments and agencies in discharging these responsibilities, including the Departments of State, Justice, and Labor.

Multiple components within DHS share responsibility for executing immigration and visa policy. CBP, ICE, and U.S. Citizenship and Immigration Services (USCIS), along with USCG, the US-VISIT program within NPPD, and other organizational elements execute these responsibilities. Strengthening and effectively administering immigration services and adjudicative decisions—



whether they include determinations of eligibility, admissibility, or removability—requires collaborative efforts by all partners.

DHS, through USCIS, provides immigration and naturalization benefits, as well as asylum and other services to immigrants. The Citizenship and Immigration Services Ombudsman in DHS headquarters works to improve the delivery of immigration and citizenship services and assists the public in resolving difficult cases.

USCIS plays the principal role in adjudicating immigrant and nonimmigrant visa petitions, applications for adjustment of status, and requests for extensions of stay for tourists, students, business visitors, and other visitors. In addition, USCIS adjudicates applications for asylum and refugee status, petitions for intercountry adoption, and administers immigration benefits for other vulnerable populations such as victims of human trafficking, violent crimes, armed conflict, environmental disaster, and domestic violence. Effective administration of the immigration system depends on ensuring that immigration decisions are fair, lawful, and sound. In addition, the Department works with communities, other Federal departments and agencies, and nongovernmental organizations to promote the integration of lawful immigrants into American society. USCIS works with the Departments of Health and Human Services, Labor, State, and Housing and Urban Development on issues with overlapping jurisdiction.

#### Preventing Unlawful Immigration

In addition to administering the immigration system, DHS plays the lead role in preventing unlawful immigration. These activities include DHS's efforts to effectively secure U.S. air, land, and sea borders (discussed above), while removing foreign nationals who pose national security-related and other threats to the United States, or who are otherwise in the United States illegally.

ICE, working with USCIS and CBP, also plays a key role in preventing unlawful immigration through its investigative, intelligence, deterrence, and enforcement functions. But because barriers, screening, and enforcement operations alone cannot completely stop illegal immigration, systematic efforts to reduce the jobs magnet are necessary. Employers continue to hire workers who are not authorized to work—some knowingly and others unknowingly—because workers present fraudulent documents. Recent technological advances have improved identification of fraudulent documents and provide employers with tools to verify the work authorization status of newly hired employees.

DHS works to reduce demand for illegal immigrants by conducting inspections, audits, and investigations of employers who hire illegal immigrants and administers tools such as E-Verify and the Systematic Alien Verification for Entitlements (SAVE) system to facilitate compliance with immigration laws. The Department also works to eliminate systemic vulnerabilities by combating fraudulent applications for immigration services and by investigating fraudulent use of immigration documents to obtain other benefits or government services.

DHS works to prevent illegal entry by partnering with the Department of State both domestically and overseas to ensure that visas to enter the United States are not granted to foreign nationals who pose a threat to public safety or national security. These efforts complement U.S. border

security efforts that prevent illegal entry both at and between ports of entry, described in the above section. DHS also works closely with the Departments of Justice and State as well as foreign governments and nongovernmental partner entities to share information used to combat alien smuggling and human trafficking.

Finally, ICE administers the detention and removal system by which foreign nationals found to be national security or public safety threats, criminals, or otherwise unlawfully present in the United States are arrested, detained, and removed from the United States. The Department works with the Department of Justice to ensure timely hearing of immigration cases and appeals, and with the JTTF with respect to foreign nationals who pose a national security threat.

Although immigration enforcement is constitutionally vested with the Federal government, DHS partners with State, local, tribal, and territorial law enforcement officers through the Secure Communities program to assist in identifying criminal foreign nationals and foreign nationals posing national security threats who are incarcerated. In addition, under the INA's Section 287(g) program, State, local, tribal, and territorial law enforcement agencies are granted limited authority, under Federal supervision and monitoring, to enforce Federal immigration laws.

#### *Initiatives and Enhancements*

The QHSR and BUR analyses make clear that achieving success in enforcing and administering our immigration laws will demand enhanced policies, targeted enforcement, and improved management of the system. Comprehensive legislative reform remains a fundamental necessity. We must continue to move beyond a paper-based application process and seek ways to standardize services, policies, and implementation throughout the system. Our ability to quickly analyze information, identify high-risk cases, and focus on fraud and national security concerns must continue to improve. We must continue to improve E-verify and find ways to promote and incentivize voluntary employer compliance. We must address fundamental issues related to our detention and removal efforts and build the detention system commensurate with the risk. Finally, new Americans need greater opportunities to become full members of their communities.

Based on DHS' responsibilities in this area, DHS will pursue comprehensive immigration reform, improve DHS immigration services processes, focus on fraud detection and national security vetting, target egregious employers who knowingly exploit illegal workers, dismantle human smuggling organizations, improve the detention and removal process and emphasize Secure Communities and efforts to identify and deport criminal aliens, ensure the integration of our newest Americans so that they become fully vested members of our Nation, and build and maintain a model detention system.

- *Comprehensive immigration reform.* Effective enforcement and administration of our immigration laws can best be built on comprehensive legislative reform that: (1) bolsters border security and interior enforcement; (2) mandates a nationwide employment verification program to stem the demand for illegal immigration and hold employers accountable for hiring unauthorized workers; (3) provides a mechanism to help clear family and employment visa backlogs; (4) recasts the legal migration provisions to better

match the needs of the twenty-first century, for both high-skill and low-skill workers; and (5) carefully crafts a tough but fair program under which illegal immigrants will register, record biometrics, pass a criminal background check, pay any back taxes, pay a fine, learn English, and in return, be allowed to remain legally in the country and earn the opportunity for lawful permanent residence. Working closely with interagency partners and Congress, and in ongoing dialogue with external stakeholders from across the country, DHS will continue to develop and advance comprehensive immigration reform legislation.

- *Improve DHS immigration services processes.* Effective administration of the immigration system depends on fair, user-friendly processes and the identification and correction of vulnerabilities in real time. DHS will expedite the transformation of the immigration services system from a paper-based to an electronic-based application process. The Department will also ensure the standardization of immigration services policies and implementation across regions, offices, and agencies where applicable. DHS will also explore restructuring funding for USCIS to address variability in demand.
- *Focus on fraud detection and national security vetting.* DHS immigration authorities are powerful tools used against terrorists and other foreign nationals posing national security threats. DHS will improve its ability to analyze information, especially in identifying high risk cases, to better address fraud and national security concerns. DHS will strategically prioritize and manage investigations of interior immigration violations and visa overstays to target and remove criminal aliens and foreign nationals who pose a threat to national security, and increase intelligence relating to analysis of entry, exit, and stay information.
- *Target egregious employers who knowingly exploit illegal workers.* Preventing unlawful immigration depends in part on reducing the demand for illegal labor. DHS will seek legislative authority to increase civil and criminal penalties for employers who knowingly employ illegal aliens. Enhancing and expanding the E-Verify system is a critical component of ensuring a legal workforce. Additional work is underway to improve the accuracy of the system, combat identity fraud, address employer misuse, ensure that employees understand their rights, and allow employees to correct government records. While implementing E-Verify improvements and enhancing efforts to promote voluntary employer compliance, DHS will focus worksite enforcement on egregious employers who knowingly exploit illegal labor and critical infrastructure sites.
- *Dismantle human smuggling organizations.* Illegal immigration is facilitated by transnational criminal organizations that smuggle aliens internationally, across U.S. borders and within the interior of the country. DHS will enhance efforts to conduct investigations to dismantle these criminal organizations and will work with the Department of Justice to ensure successful prosecution of their leadership and forfeiture of their profits and other non-monetary assets or infrastructure. DHS will also work with the Department of Health and Human Services and other partners to implement best practices for processing undocumented, unaccompanied alien children who present themselves at the border.

- *Improve the detention and removal process.* As described above, DHS administers the detention and removal process through ICE in partnership with the Department of Justice. To improve the efficiency of this process, particularly as applied to criminal and other dangerous foreign nationals, DHS will increase non-investigatory law enforcement staffing for detention and removal operations to focus law enforcement on criminal investigations. DHS will continue to institutionalize the Secure Communities program to ensure enforcement resources are targeted based on risk, ensuring that criminal aliens are identified and processed efficiently for removal. DHS will also expand the Criminal Alien Program (CAP) at State, local, tribal, and territorial detention facilities to increase the number of criminal aliens who have removal orders by the time they complete their criminal sentence, removing the burden in detaining these aliens beyond their criminal sentences while awaiting removal orders. DHS will also seek to strengthen staffing at existing CAP sites, equip additional sites, and will work with DOJ to ensure that State, local, tribal, and territorial receipt of Federal detention funding is tied to participation in the Secure Communities (also known as a Comprehensive Plan to Identify and Remove Criminal Aliens (CIRCA)) and CAP programs.
- *Work with new Americans so that they fully transition to the rights and responsibilities of citizenship.* Effective integration of lawful immigrants supports an America where all individuals are secure in their rights, can exercise their civil liberties, and have opportunities to become full participants in their communities. Promoting integration also fosters a resilient public resistant to the enticements of extremism. DHS, with our interagency partners and stakeholders, will develop strategies that help new citizens integrate and assist eligible immigrants with naturalization. This includes core programs already underway in the public and nonprofit sectors, such as those provided by the Departments of Education and Health and Human Services. DHS will also increase its efforts to encourage legal permanent residents to become naturalized American citizens.
- *Maintain a model detention system commensurate with risk.* DHS will operate its detention system to ensure that the level of detention is commensurate with the risk posed by the detainees in its custody. Together with its partners and stakeholders, DHS will revise national standards for detainee care and treatment, including the treatment of families, minors, and those needing continuing medical treatment, ensure that detention facilities housing immigration detainees meet or exceed these standards, and cancel the contracts at facilities that receive deficient ratings. DHS will also take other steps in the near and long term to materially improve the immigration detention system. Those steps include: reducing the number of facilities DHS uses, issuing requests for proposals for new facilities commensurate with the risk posed by detainees, developing a detainee locator system to maximize communication between detainees and their families, strengthening the system that monitors the conditions within detention facilities, and ensuring the detainee health care system provides detainees with adequate and timely access to necessary care. DHS will also support increased funding for Alternatives to Detention (ATD).

#### **D. Safeguarding and Securing Cyberspace**

##### *Current Authorities*

As noted above, pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security is responsible for coordinating overall efforts to manage risk to critical infrastructure and key resources, including enhancing non-Federal cybersecurity. Homeland Security Presidential Directive 23, Cybersecurity Policy, provides that the Secretary shall lead the national effort to protect, defend, and reduce vulnerabilities of Federal systems (excluding civilian national security systems), and shall provide consolidated intrusion detection, incident analysis, and cyber response capabilities to protect Federal agencies' external access points. The May 2009 Cyberspace Policy Review outlined specific cybersecurity responsibilities to DHS. Additionally, the U.S. Secret Service is authorized by law to prevent, detect, and investigate electronic financial crimes, working closely with state and local law enforcement. The support for the Department's cybersecurity efforts is also embedded in the missions of Intelligence and Analysis, Science and Technology, and other offices and components.

##### *Overview of the DHS Role*

Cyber infrastructure forms the backbone of the Nation's economy and connects every aspect of our way of life. While the cyber environment offers the potential for rapid technological advancement and economic growth, a range of malicious actors seek to exploit cyberspace for dangerous or harmful purposes, disrupt communications or other services, and attack the Nation's infrastructure through cyberspace. We must secure the system of networks and information while promoting economic growth, protecting privacy, and sustaining civil rights and civil liberties.

##### Creating a Safe, Secure, and Resilient Cyber Environment

DHS leads the national effort to protect civilian government computer systems, in cooperation with the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). DHS also works with industry to defend privately-owned and operated critical infrastructure and with State, local, tribal, and territorial governments to secure their systems.

To protect against current threats, DHS has the primary responsibility for working with civilian agencies and cyber centers across the Federal government, with State, local, tribal, and territorial governments, and with the private sector, to share information and collaborate to enable understanding of the threat, provide indications and warnings, and create common situational awareness utilizing and strengthening the public private partnership model established under the *National Infrastructure Protection Plan*. DHS collects and analyzes a wide variety of information regarding current and emerging cybersecurity threats and threat actors, and disseminates products to help improve the defensive posture of Federal agencies. DHS operates the National Cybersecurity and Communications Integration Center, which receives and analyzes reports of cyber incidents on Federal agency networks and provides warnings to Federal agencies, State, local, tribal, and territorial governments, and critical infrastructure owners and

operators. DHS also operates the National Cyber Security Center, which promotes coordination and common situational awareness across Federal cybersecurity operations centers. Working through the councils of the *National Infrastructure Protection Plan's* Sector Partnership, other Critical Infrastructure Partnerships and their unified public-private Information Sharing Environment, DHS, other Federal agencies, and State, local, tribal, and territorial governments, collaborate and share cybersecurity information with critical infrastructure owners and operators, to enhance understanding of the threat, situational awareness, prevention, and incident response. DHS also maintains an area of focus on the security of control systems, which manage the basic functions of significant elements of our infrastructure, in order to further resilience.

Similarly, DHS has the responsibility to support cyber risk management and reduction in the Federal civilian (excluding civilian national security systems) and State, local, tribal, and territorial government domains as well as in the private sector, to support their efforts to protect information systems, networks, personal and sensitive data, and to make systems and networks more resilient. Through the Trusted Internet Connection, EINSTEIN, and other programs, DHS is strengthening the defenses of Federal agency networks and enhancing protection of privacy by reducing their exposure to attacks, setting standards for security and network operations centers, and deploying intrusion sensors to detect and prevent attacks. In cooperation with the Department of Commerce and OMB, DHS develops and issues advisories and best practices to Federal agencies, helping to ensure that known vulnerabilities are addressed quickly and that preparations are made to mitigate emerging threats. Going forward, DHS will continue to support Federal civilian agencies and the private sector in meeting national and homeland security-related cybersecurity requirements—derived from standards, policy, and an understanding of the threat and necessary responses.

DHS is responsible for creating and maintaining a robust public-private cyber incident response capability to manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action. DHS is responsible for coordinating effective response by Federal civilian agencies—as well as military and intelligence agencies as appropriate—and where necessary, directing appropriate mitigation; DHS also supports and coordinates with the private sector to enhance its response. To serve many of these purposes, DHS maintains the United States Computer Emergency Readiness Team (US-CERT), which is charged with providing response support and defense against cyber intrusions and attacks for Federal civilian networks (excluding civilian national security systems) as well as information sharing and collaboration with State, local, tribal, and territorial governments, industry, and international partners. US-CERT interacts with Federal agencies, industry, the research community, State, local, tribal, and territorial governments, and others to disseminate reasoned and actionable cybersecurity information to the public. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about cybersecurity. DHS works closely with civilian, military, law enforcement, and intelligence agencies to ensure an integrated and holistic response.

DHS shares responsibility with other government agencies to prevent cyber crime and other malicious uses of cyberspace, by disrupting criminal organizations and other bad actors engaged in high-consequence or wide-scale cyber crime. DHS law enforcement components—particularly USSS and ICE—play key roles in investigating, disrupting, and deterring homeland

security-related cyber crime, specifically, high-consequence or wide-scale crimes committed in cyberspace or against cyber networks, particularly in the financial, child exploitation, and intellectual property arenas, respectively, working closely with other Federal agencies and State, local, tribal, territorial, and international partners to disrupt criminal activity affecting U.S. assets. USSS has established a network of 29 domestic and international Electronic Crimes Task Forces (ECTF) to combine the resources of academia, the private sector, and Federal, State, local, tribal, and territorial law enforcement agencies to combat computer-based threats to U.S. financial systems and critical infrastructure—a capability that has allowed ECTFs to identify and address potential cyber vulnerabilities before criminals exploit them. ICE's Cyber Crimes Center investigates cyber crimes involving cross-border criminal activity, including child exploitation, identity, document, and benefit fraud, thefts of intellectual property, money laundering, commercial fraud, counterproliferation, and other cross-border criminal schemes.

In its efforts to promote cybersecurity, DHS benefits from the work of its Privacy Office and its Office for Civil Rights and Civil Liberties. For example, the Privacy Office has conducted, and made available to the public, reviews of the EINSTEIN program. Likewise, the Privacy Office has conducted a classified Privacy Impact Assessment of the exercise involving enhanced capabilities for the EINSTEIN program and information-sharing with the National Security Agency, and has made available to the public an unclassified version of that assessment in furtherance of the DHS commitment to transparency. Through the continuing work of these offices, DHS will ensure that the initiatives it undertakes to promote cybersecurity will protect privacy, civil rights, and civil liberties.

#### Promoting Cybersecurity Knowledge and Innovation

To protect against future threats, and to create a more secure cyber “ecosystem,” DHS works broadly to raise awareness, build knowledge, drive innovation, and create the technical and governance foundation of stronger network security. DHS will also lead the Administration's National Cybersecurity Public Awareness Campaign, and is working with other Federal departments and agencies to build the cyber workforce of the future.

DHS plays a key role in supporting innovation by sponsoring technical and other research in the public and private sectors. Perhaps most important, as part of DHS' responsibility to enhance the protection of critical infrastructure, including the government, DHS is driving efforts to make the cyber ecosystem more secure by building standards and governance solutions that meet national and homeland security requirements. This includes automation of security to facilitate real-time response, interoperability to support security cooperation across sectors, and privacy-enhancing authentication so we can effectively protect our systems.

DHS, in partnership with the private sector, State, local, tribal, and territorial governments, and Federal agencies such as the Departments of Defense and Commerce, also encourages the enhancement of the security and integrity of the hardware, software, services, and architecture that will constitute a fundamentally more secure cyber ecosystem. DHS also supports research and development of emerging cybersecurity products and processes, working closely with industry and academia to bring promising new technology and techniques to increase the Nation's cybersecurity.

### *Initiatives and Enhancements*

Given DHS's broad responsibility for Federal civilian (excluding civilian national security systems) and private sector networks and the priorities outlined in the QHSR, DHS's cybersecurity activities must be consolidated, coordinated, and strong. The line between physical and cyber critical infrastructure continues to blur, creating synergies across these activities that must be accounted for when considering our organizational and operational posture. Cybersecurity authorities across the Federal government have in many cases adapted well to a more networked world, but work remains to ensure clear lines of authority and mission. Adversaries continue to shift and refine tactics to penetrate our networks, placing high demand on our ability to anticipate, attribute, and prosecute cyber threats. Finally, though much progress has been made, efforts to maintain strong public awareness of the latest tactics and techniques and the optimal means of thwarting them must be continuously honed and improved.

For these reasons, DHS will undertake the following initiatives and enhancements to strengthen the Department's capabilities in cybersecurity—including creating a cybersecurity and infrastructure resilience operational component within DHS, strengthening DHS authorities and capabilities to protect cyber networks, increasing DHS cyber predictive, investigative, and forensic capabilities, and promoting cybersecurity public awareness.

- *Increase the focus and integration of DHS's operational cybersecurity and infrastructure resilience activities.* DHS has substantial operational cyber security responsibilities, which are inextricably intertwined with its responsibilities to manage all hazards risk to critical infrastructure. DHS typically manages its operational responsibilities through operating components. However, the majority of DHS's operational activities relating to cyber security and infrastructure protection and resilience are currently administered by the NPPD, which is designated as a DHS headquarters element. DHS will focus NPPD's activities on operations and more closely align cyber and critical infrastructure protection and resilience efforts, in cooperation with the private sector, to secure cyber networks and make critical infrastructure resilient. DHS will examine ways to clarify NPPD's increasingly operational role as opposed to other elements of the DHS headquarters, as well as NPPD's functions not related to cybersecurity or infrastructure protection and resilience.
- *Strengthen DHS ability to protect cyber networks.* DHS is responsible for the protection of Federal networks (the .gov domain), excluding civilian national security systems. However, further efforts are needed to effectively fulfill this responsibility. To this end, DHS will increase its cybersecurity activities for Federal civilian networks (excluding civilian national security systems) to ensure that national cybersecurity requirements are met, as well as additional resources to develop the capabilities necessary to effectively implement those authorities in close collaboration with other departments and agencies. In order to keep pace with emerging threats and new technologies, DHS will also seek to use new models for developing, acquiring, and disseminating cybersecurity technology, including technology leasing arrangements, technical service agreements, and development of secondary markets for cybersecurity technology among State, local,



tribal, and territorial governments. Finally, DHS' effort to "design-in" greater resilience for critical infrastructure to ensure national security requirements are met will include a cybersecurity focus.

- *Increase DHS predictive, investigative, and forensic capabilities for cyber intrusions and attacks.* The ability to predict the emergence of new cyber threats will help mitigate the effects of such threats. Likewise, the ability to determine the source of a cyber attack, intrusion, or disruption both increases the likelihood of a successful prosecution of the attacker and creates a powerful deterrent effect against both state and non-state actors. To that end, DHS will build a new predictive analytic capability that will work closely with the law enforcement and intelligence communities and the private sector to improve the identification of cyber adversaries, establish and advance deterrence strategies, and promote a more accurate understanding of emerging cyber threats. To meet these goals, DHS will enhance its efforts to recruit and develop an expanded cyber intelligence and analysis team. DHS will also expand and prioritize investigative activities targeted at high-consequence or wide-scale cyber attacks, intrusions, and disruptions, and associated transborder cybersecurity-related crime, in cooperation with other law enforcement agencies through the National Cyber Investigative Joint Task Force. DHS will establish reliable mechanisms to categorize, store, and retrieve relevant cyber information from DHS databases, consistent with protection of privacy, civil rights, and civil liberties. Finally, DHS will develop and implement a robust process to share finished cyber intelligence products and other information in a timely fashion within DHS and with our Federal, State, local, tribal, territorial, and private sector partners.
- *Promote cybersecurity public awareness.* As the President's Cyberspace Policy Review found, people cannot value security without first understanding how much is at risk. Therefore, DHS will enhance its own cybersecurity awareness program and continue to lead the national cybersecurity public awareness campaign aimed at individual users of the Internet, as part of the Administration's National Initiative for Cybersecurity Education. This campaign will empower and support citizens and organizations to use the Internet securely and safely, protecting themselves and the cyber infrastructure.

## **E. Ensuring Resilience to Disasters**

### *Current Authorities*

DHS's role in ensuring resilience to disasters is shaped primarily by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), the Post Katrina Emergency Management Reform Act (PKEMRA), and other Executive Orders and Congressional mandates. The Homeland Security Act of 2002 identifies as primary mission of the Department the responsibility to act as a focal point regarding natural and manmade crises and emergency planning. Under Title V of the Homeland Security Act, as amended by PKEMRA, the Secretary of Homeland Security, through the FEMA Administrator, is responsible for leading the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents. The Stafford Act is the Nation's primary authority for all-hazards emergency

management; the FEMA Administrator exercises a variety of authorities under the Stafford Act on behalf of the President and the Secretary of Homeland Security. Homeland Security Presidential Directives 5, 8, and 20 make the Secretary of Homeland Security responsible for domestic incident management and national preparedness, and national continuity operations and activities, respectively; these functions are largely carried out by FEMA. Statutes such as the National Flood Insurance Act of 1968, the Earthquake Hazards Reduction Act of 1977, and the National Dam Safety Program Act vest FEMA with significant hazard mitigation authorities. The Implementing the Recommendations of the 9/11 Commission Act of 2007 codify several of the Department's preparedness grant programs. The Federal Fire Prevention and Control Act of 1974 vests FEMA with a variety of fire prevention, preparedness, and response authorities. Further, the Ports and Waterway Safety Act of 1972, amended by the Port and Tanker Safety Act of 1978, authorizes the USCG to establish requirements for vessels and other port safety controls, to minimize threats to the safety and security of U.S. citizens, facilities, vessels, national assets, and the environment. The Comprehensive Environmental Response, Compensation, and Liability Act, the Superfund Act, and the Oil Pollution Act of 1990 establish broad Federal authority to respond to releases or substantial threats of releases of oil and hazardous substances; these authorities are executed by the U.S. Coast Guard in conjunction with the Environmental Protection Agency.

#### *Overview of the DHS Role*

Ensuring domestic resilience to disasters is grounded in the four fundamental elements of emergency management: mitigating hazards, increasing our Nation's preparedness, effectively responding to emergencies, and supporting community recovery. The QHSR also highlighted the overarching importance of resilience to the Nation's ability to withstand and recover from disasters. To that end, DHS will foster an approach to disaster management nationally that is built upon a foundation of proactive engagement at the community level that builds community resilience and supports local emergency management needs.

During domestic disasters, the Department's role, largely executed through FEMA, is principally one of coordinator, working closely with our State, local, tribal, and territorial partners, as well as nongovernmental organizations and the private sector, to enhance preparedness, build and sustain capabilities, and act as an aggregator of resources from across the Federal government. DHS, through FEMA, also has specific direct responsibilities, including disaster response and field coordination, disaster logistics, individual and public assistance programs, as well as the lead coordinating role for national continuity programs. DHS maintains significant first responder and coordination capabilities for disasters in the maritime domain through USCG with its broad Captain of the Port authority and role as Federal Maritime Security Coordinator and Federal On-Scene Coordinator in the coastal zone. USCG provides multi-mission surface, air, and shore assets that take action to save lives, minimize damage, and protect the environment. DHS, through the National Protection and Programs Directorate, also ensures the resilience of critical infrastructure to disasters.

#### Mitigating Hazards

DHS is uniquely positioned not only to support communities during a disaster, but also enable State, local, regional, tribal, and territorial partners to take steps that will decrease risk and mitigate future hazards before a disaster strikes. DHS works closely with our local and regional partners to identify hazards, assess vulnerabilities, and develop strategies to manage the risks associated with natural and man-made hazards. The Department works to reduce risk to life and property through encouraging land use controls and adoption of building codes, while also applying engineering and planning practices in conjunction with advanced technology tools. A primary area of focus is reducing flood loss and damage, by ensuring that communities across the country have access to affordable flood insurance while also encouraging communities to adopt and enforce floodplain management regulations that mitigate the effects of flooding. DHS also enhances structural resilience through interrelated stewardship and safety responsibilities, particularly in the maritime sector.

#### Enhancing Preparedness

Increasing preparedness is a key responsibility of DHS. This responsibility includes working collaboratively to increase the preparedness of our State, local, regional, tribal, and territorial partners, as well as nongovernmental organizations, the private sector, and the general public. DHS has responsibility for crafting a national preparedness goal and system and building preparedness capabilities through planning, training, safety and security standards, technical assistance, exercises and credentialing for homeland security partners and stakeholders at all levels of government and industry. The primary vehicle for enhancing preparedness at the State, local, regional, tribal, and territorial level are grant programs—notably the State Homeland Security Grant Program and Urban Areas Security Initiative—which along with other grant programs collectively provide almost \$4 billion annually to State, local, regional, tribal, and territorial governments. The Department is also the lead in providing guidance and resources to aid in building preparedness at the local and regional level by encouraging individuals and families, the private sector and community-based organizations to reduce vulnerabilities and improve their capacity to withstand disasters through planning, readiness, and capacity-building activities. To this end, DHS works closely with local and regional officials and first responders encouraging public preparedness activities and awareness campaigns, and works with a number of national networks of community based preparedness teams. Federally-administered training programs—such as FEMA’s National Domestic Preparedness Consortium, Emergency Management Institute, and Center for Domestic Preparedness—also play a critical role in developing the knowledge, skills, and abilities of stakeholders in the private sector and at all levels of government. DHS, through USCG, establishes and enforces safety and security regulations on mariners, vessels, and maritime facilities to ensure all-hazard preparedness. Finally, DHS improves catastrophic preparedness through the establishment of shared preparedness and response objectives and planning for responding to extreme events.

#### Ensuring Effective Disaster Response

DHS, primarily through FEMA, acts as the Federal coordinator during disaster response, supporting State, local, regional, tribal, and territorial governments while working closely with

nongovernmental organizations and the private sector to help leverage the resources that they can bring to bear. This coordination ensures that our Nation's emergency response is functioning in a comprehensive, unified manner. To meet disaster response requirements, FEMA maintains Incident Management Assistance Teams, the National Urban Search and Rescue Response System, Mobile Emergency Response Support Detachments, the National Response Coordination Center and a network of Regional Response Coordination Centers, disaster emergency and interoperable communications capabilities, a robust disaster logistics capability, and recovery programs to provide public assistance and individual assistance to affected citizens. DHS, through FEMA, also disseminates emergency alert information during an emergency through the Integrated Public Alert and Warning System (IPAWS) which is designed to provide a multi-faceted dissemination mechanism for alerts beyond traditional audio-only and television warnings. The IPAWS program leverages technological advancements in how messages can be disseminated as well as how, and on what types of devices, they can be received in the event of an emergency. Through USCG, DHS also maintains robust multi-mission first responder assets capable of saving lives, protecting property and the environment, and responding to all-hazards disasters within the maritime domain. USCG, together with the Environmental Protection Agency, coordinates the response to Spills of National Significance under the National Contingency Plan for oil and other hazardous materials spills in navigable waterways.

#### Supporting Community Recovery

DHS plays a key role in facilitating community recovery following a disaster. Through FEMA's Public Assistance and Individual Assistance programs, DHS is able to support eligible reconstruction projects and provide eligible disaster survivors with financial support as they begin the road to recovery. In conjunction with the Small Business Administration and the Departments of Housing and Urban Development, Agriculture, and other Federal agencies, the Department also provides State, local, tribal, and territorial governments with access to subject matter experts to assist local governments with planning and coordinating the rebuilding efforts. In addition, FEMA serves in a key role to ensure government-wide continuity of operations in the event of a disaster. USCG "first responder" assets quickly become recovery platforms following a maritime disaster and play critical roles in restoring the Maritime Transportation System and the flow of commerce through our ports and waterways. USCG and CBP have substantial responsibilities for facilitating the restoration of trade following a major disruption due to disaster.

The devastating effects of recent disasters have highlighted the need to reform our national approach to long-term recovery. Communities devastated by a disaster, particularly large-scale and catastrophic events such as Hurricane Katrina face complex and difficult challenges, including restoring economic viability, rebuilding infrastructure and public services, and establishing resilience against future hazards. To that end, in September 2009, the President directed DHS and the Department of Housing and Urban Development (HUD) to co-chair an interagency working group to strengthen long-term disaster recovery at the Federal, State, local, tribal, and territorial levels. Following an extensive outreach effort with stakeholders across the country, this effort will result in two documents in 2010: a National Disaster Recovery Framework (NDRF) and a report to the President with specific recommendations to improve the Nation's capacity for effective long-term recovery. The NDRF, a companion document to the

National Response Framework, will outline how community recovery is supported on a national level. The report to the President will recommend improvements to the way in which government at all levels, the private sector, non-profit organizations, communities, and individuals prepare for and recover from a disaster. DHS's efforts, through FEMA, will include a particular focus on enhancing the delivery of recovery support functions for which FEMA is directly responsible, such as funding for public infrastructure rebuilding.

#### *Initiatives and Enhancements*

The QHSR and BUR analyses show that DHS's responsibilities in disaster resilience require enhanced planning, management systems, resilience policies, and the promotion of individual, family and community preparedness. Planning for catastrophic disasters must be more coordinated and predicated on nationally agreed-upon, risk-based preparedness standards. FEMA personnel must be developed to further enhance DHS's ability to lead in emergency management. DHS must lead non-governmental sectors in setting infrastructure design standards and get expanded authority to regulate high-risk assets. Finally, new mechanisms are needed to enhance preparedness at the community, family, and individual levels.

Therefore, DHS will undertake the following initiatives and enhancements to enhance catastrophic disaster preparedness, improve DHS' ability to lead in emergency management, explore opportunities with the private sector to "design-in" greater resilience for critical infrastructure, and make individual and family preparedness and critical facility resilience inherent in community preparedness.

- *Enhance catastrophic disaster preparedness.* Of particular importance to DHS is our national preparedness for catastrophic events. National efforts to ensure resilience to these events must focus on improving existing catastrophic preparedness. This requires close collaboration with all partners to establish shared objectives and capability standards at the Federal, State, local, regional, tribal, territorial, nongovernmental, and private sector levels. We must engage and integrate the public as part of the solution to achieving greater overall catastrophic preparedness. Planning assumptions must address risk-based worst case scenarios (maximums of maximums) with resource thresholds that are intended to challenge preparedness at all levels of government. These scenarios will enable planners to seek innovative, non-traditional solutions to catastrophic events. Partnerships in planning for these events will also extend beyond the traditional coalitions, that involve Federal, State, local, regional, tribal, territorial, community planners, the private sector, and nonprofit organizations. Plans will be supported by training, technical assistance and grants, and ultimately be validated through robust exercises designed to overload the system so additional capability shortfalls can be identified and addressed.
- *Improve DHS' ability to lead in emergency management.* To improve overall effectiveness in emergency management, FEMA will create a new strategic approach to developing the agency's current workforce, recruiting and hiring the best talent available and strengthening skill sets across the workforce in support of FEMA's core responsibilities. DHS will create a career path for employees with emergency

management responsibilities, including headquarters positions, field deployments, and mobility assignments, and implement both paid and unpaid internship programs to develop future emergency managers. FEMA will implement personnel exchanges between headquarters and regional offices to enhance employee understanding of headquarters and regional perspectives, as well as personnel exchanges between FEMA and State governments through the Intergovernmental Personnel Act. DHS will reassess, refine, and clarify roles and responsibilities for emergency management through the *National Response Framework* revision process, which will help streamline the delivery of effective disaster response. DHS will also promote access to emergency management-related information by homeland security partners and stakeholders, in order to promote a shared understanding of how risks are prioritized and managed and inform resource allocation decisions. Finally, DHS will align FLETC State, local, regional, tribal, and territorial law enforcement with training through FEMA's National Domestic Preparedness Consortium, Emergency Management Institute, and Center for Domestic Preparedness in order to harmonize curriculums and take advantage of complementary learning experiences. DHS will also enhance coordination of existing fellowship programs that receive DHS support to ensure coordination and maximize the effectiveness and utility of those programs.

- *Explore opportunities with the private sector to “design-in” greater resilience for critical infrastructure.* Our efforts to reduce vulnerabilities to critical infrastructure and key resources must include not only physical protection measures but also inherent resilience. It is more efficient and more effective to build in resilience by design than to retrofit for resilience once facilities and networks are developed. To that end, DHS will work with nongovernmental organizations that set infrastructure design standards to establish commonly-agreed standards for critical infrastructure resilience. DHS will build upon the standards adoption authority provided under Title IX of the Implementing the 9/11 Recommendations Act of 2007, and will seek to incorporate design standards for critical infrastructure resilience into Federally-administered insurance and re-insurance programs. DHS will also examine the need to set security requirements at high-risk assets and in high-risk areas as appropriate, and to set standards for security practices in critical infrastructure sectors as necessary. Finally, DHS will seek to obtain information from the private sector with protections preventing such information from unnecessary disclosure, in order to allow DHS to make determinations concerning risk.
- *Make individual and family preparedness and critical facility resilience inherent in community preparedness.* Preparedness and hazard vulnerability reduction must be inherent in communities in the same way that protection and resilience must be built into critical infrastructure by design. DHS will work with its Federal, State, local, tribal, territorial, nongovernmental, and private sector partners to develop new mechanisms for building in preparedness and hazard vulnerability reduction into urban planning, community-provided education, and civic organizations.

#### **F. Complementary Department Responsibilities and Hybrid Capabilities**

DHS also performs a number of services and functions that are complementary to its homeland security mission responsibilities, including marine safety, stewardship, and environmental protection and certain categories of law enforcement activities. These services and functions are typically performed with hybrid capabilities—assets and resources capable of performing multiple missions—which are a hallmark of homeland security. For example, the same assets and personnel that patrol our borders, enforce our immigration laws, and respond to major oil spills also enforce safety regulations, assist travelers, and safeguard natural resources. These complementary activities are critical to fulfilling other national interests, and are often intertwined with and mutually supporting of homeland security activities.

#### **IV. Improving Department Management**

As noted earlier, the integration of all or part of 22 different Federal departments and agencies into a unified, integrated Department of Homeland Security continues to represent a significant public policy and management challenge. In its seven years of existence, DHS has taken significant steps to create a unified and integrated Department, and the bottom-up review process has provided a unique opportunity to examine and improve the way the Department runs itself.

##### *The DHS Efficiency Review*

To unify the Department, the Secretary launched a major initiative to foster a culture of responsibility and fiscal discipline, cut costs, and streamline operations through a series of measures that are expected to lead to significant cost avoidances. Since its launch in March 2009, the DHS Efficiency Review program has implemented nearly two dozen separate initiatives to achieve these aims while also promoting greater accountability, transparency, and customer satisfaction. The Efficiency Review has led to improvements in how the Department manages its resources in several areas, including its physical assets and support of its workforce, as well as the day-to-day expenditures required to do business. As part of the Efficiency Review and through other channels, DHS has also made improvements in how it supports its workforce. An expanded discussion of Efficiency Review initiatives is set forth at Annex C to this report.

##### *A DHS International Engagement Framework*

The flow of people and goods around the world and across U.S. borders can advance America's interests, but can also create security challenges that are increasingly borderless and unconventional. Within this environment, DHS has a core responsibility to ensure the safety, security, and resiliency of the United States and the global trade and travel systems upon which our Nation relies.

In order to fulfill its full range of missions, DHS must build on U.S. international partnerships to enhance our ability to identify vulnerabilities and to understand, investigate, and interdict threats at the earliest possible point, ideally before they become manifest, reach our shores, or disrupt the critical networks on which we depend. To that end, DHS will be developing a strategic framework for DHS international engagement to provide common policy objectives and

priorities across the Department. The framework will prioritize the Department's engagement, activities, and footprint abroad, and advance DHS's ability to meet future challenges around the world. This international framework will be consistent with the broad range of U.S. Government international priorities and in consultation and coordination with the Department of State and the U.S. Chiefs of Mission in foreign countries.

The DHS international engagement framework will focus on the following areas of emphasis:

- Increased cooperation with international partners to identify, prevent, deter, investigate, and disrupt threats, and manage homeland security risks through dynamic information and knowledge sharing and cooperation in joint operations;
- Enhanced collaboration with international partners to develop norms, standards, and regulatory environments that enhance international security activities relating to homeland security, including aviation security, maritime security, and global supply chain security;
- Enhanced collaboration with international partners in technology development and evaluation for homeland security applications; and
- Increased capacity building, training, and technical assistance in partnership with the Departments of State and Defense to strengthen weak links in the global systems that move people and goods.

#### *Initiatives and Enhancements*

The QHSR statute required an assessment of the organizational alignment of the Department with the national homeland security strategy and homeland security missions set forth in the QHSR Report. The BUR included this assessment. The assessment showed that six years since its establishment as a Federal department, there remain critical opportunities to enhance integration across DHS, including operationally by ensuring clear delineation of headquarters and operational components; aligning the multiple regional structures that exist across operational components nationally; strengthening training and career paths through emphasis on mobility and cross-disciplinary experiences; and enhancing management and functional integration. Currently, the Secretary of Homeland Security cannot reorganize DHS in the manner envisioned by the Homeland Security Act, thereby severely limiting her ability to manage the department through a rapidly evolving security environment. Though much progress has been made in adopting a risk management posture and culture across DHS, there remains work to be done in carrying out a national risk assessment and further inculcating risk management principles and priorities throughout all DHS activities. Lastly, the health and resilience of DHS employees must remain an urgent management priority, as should the conversion of contractor to government positions.

At the core of DHS operations are its seven operating components: U.S. Citizenship and Immigration Services (USCIS); the U.S Coast Guard (USCG); U.S. Customs and Border Protection (CBP); the Federal Emergency Management Agency (FEMA); U.S. Immigration and



Customs Enforcement (ICE); U.S. Secret Service (USSS); and the Transportation Security Administration (TSA).

To improve Department management, DHS proposes to restore the Secretary's reorganization authority for DHS headquarters, realign component regional configurations into a single DHS regional structure, improve cross-Departmental management and functional integration, strengthen DHS intelligence and counterintelligence capabilities, enhance the Department's risk management capability, increase coordination within DHS through cross-Departmental training, enhance the DHS workforce through more developed career paths, and increased diversity, especially at senior levels, and reduce reliance on contractors.

- *Seek restoration of the Secretary's reorganization authority for DHS headquarters.* At its founding, DHS was authorized to conduct reorganizations of Department functions upon 60 days notice to Congress, with the exception of USSS and USCG. Over time, Congress has limited that authority to a point where today the Secretary is restricted from using that authority at all. To provide the Secretary with the authority to realign the Department's headquarters to meet new threats and realize greater efficiencies, DHS will request that Congress remove current restrictions on the Department's ability to use its authority under Section 872 of the Homeland Security Act of 2002 with respect to its headquarters.
- *Realign component regional configurations into a single DHS regional structure.* Each of DHS's seven current operating components use a different regional structure for locating offices, allocating resources, and conducting operations and planning across the United States. To streamline operations nationally, increase efficiencies, and enhance cross-training and rotational assignments, DHS will align the seven separate regional structures currently in use by the operating components to a single, nationwide regional structure. DHS is currently examining the best mechanism for harmonizing and integrating its regional structure, including any recommendations regarding legislative authority necessary to effectuate such an alignment.
- *Improve cross-Departmental management, policy, and functional integration.* DHS's business chiefs (e.g. Chief Financial Officer, Chief Information Officer) conduct cross-Department management and oversight as well as perform day-to-day service functions for DHS headquarters directorates and offices. In order to improve cross-Department management, DHS will examine the creation of a Headquarters Services Division within the Management Directorate from the existing service functions of the business chiefs that will provide day-to-day business support functions to DHS headquarters elements. In order to increase cross-Departmental policy development and coordination, DHS will also seek to elevate the position of Assistant Secretary for Policy to an Under Secretary.

To transform and increase the integration of Departmental management functions, DHS is concentrating on seven specific initiatives: Enterprise Governance; a Balanced Workforce Strategy; Transformation and Systems Consolidation (TASC); Headquarters Consolidation and St. Elizabeth's; Human Resources Information Technology; Data Center Migration; and Homeland Security Presidential Directive 12 Implementation.

These initiatives will help drive transformation to a “One DHS” culture through cohesive horizontal and vertical integration and management of Department-wide initiatives, improve the transparency and functionality of critical management systems, increase cybersecurity of our networks through consolidation of data centers, effectively manage real estate in the National Capital Region, and create common identification procedures within DHS. Full implementation of Homeland Security Presidential Directive 12, including a single DHS identification card and common operating procedures and protocols for employee and contractor access, will ensure a single secure identification credential for all of DHS.

- *Strengthen internal DHS counterintelligence capabilities.* It is imperative for DHS to have an effective and coherent counterintelligence effort. DHS will enhance its counterintelligence capabilities and posture through increased training and reporting, pre-briefing and de-briefing of employees traveling abroad and recurrent vetting programs for contractor personnel. DHS will also develop a cyber counterintelligence capability to complement existing information assurance activities. In addition, DHS will address structural impediments to improving the counterintelligence function within the Department by integrating currently separated counterintelligence activities into a unified counterintelligence program.
- *Enhance the Department's risk management capability.* As the QHSR identified, ultimately homeland security is about effectively managing the risks to the Nation. Employing an integrated risk management framework, DHS will enhance its capability to inform strategies, processes, and decisions to enhance security and to work in a unified manner with its homeland security partners to manage risks. DHS will continue building this framework and invest in the governance, policy, guidance, processes, tools, training, and accountability necessary to manage risk. DHS will also continue to work to evaluate all hazards risks to the Nation, identify improved strategies for managing risks, and measure performance in terms of risk reduction.
- *Strengthen coordination within DHS through cross-Departmental training and career paths.* DHS's most valuable resource is its people. Thus, any effort to achieve a unified DHS must focus on the men and women who work at DHS. DHS will strengthen Department unity by developing DHS career paths that provide mobility within the Department and span headquarters and operational components. DHS will also increase the number of DHS component personnel on rotation in headquarters directorates and offices, and the number of DHS headquarters personnel on rotation in components. As part of interagency national security and homeland security professional development, DHS will also explore interagency and intergovernmental rotational assignments with Federal, State, local, tribal, and territorial partners.
- *Enhance the DHS workforce.* The Department's health, wellness, and resilience programs are critical to employee retention and performance. DHS has created programs such as the DHS Together Employee Initiative and the Organizational Resilience Initiative to ensure that Department employees have the tools and resources to manage the stresses inherent in these occupations. DHS also plans to implement Workplace

Wellness programs, including employee resilience training, to address the needs of the Department's diverse workforce. DHS will create a standardized, metrics-driven health program that supports the unique needs of our operational workforce, and frontline medical programs that support operational missions staffed and supported with appropriate training and equipment. DHS will also expand TSA's Idea Factory across the Department in order to harness the insights and innovations of the DHS workforce.

In addition, the Department will pursue greater diversity in its workforce, especially at senior levels. Given our critical homeland security mission, DHS must focus on the diversity of its workforce to reflect the people it serves. The Secretary recently appointed a senior-level steering committee, chaired by the Deputy Secretary, to direct a multi-year effort to promote diversity. DHS has initiated a coordinated employee recruitment initiative to improve diversity of applicant pools. This approach will emphasize targeted recruitment to increase the number of women, minorities, and veterans applying to work throughout DHS and enterprise recruitment efforts for Senior Executive Service positions. We will also deploy a Department-wide exit survey to provide more reliable information about employee attrition and to understand how this impacts diversity in the Department.

- *Balance the DHS workforce by ensuring strong federal control of all DHS work and reducing reliance on contractors.* DHS is strongly committed to a full re-examination of its workforce needs and its current reliance on contractors. In 2009, all DHS directorates, components, and offices were directed to examine current contracts and develop initial contractor conversion plans. Over the past year, the Department has been actively converting contractor positions to government positions. DHS will continue to build on these efforts at an even more aggressive pace to put in place the appropriate federal workforce required to oversee and carry out its mission responsibilities.

## V. Increasing Accountability

To enhance mission performance and improve Departmental management, DHS must increase accountability across the organization. While accountability cuts across all aspects of the organization's operations, our initial focus will be to maximize the performance and resource data we collect to inform strategic and risk-informed decision-making.

### *Data and Performance Management*

Seven years of Departmental operation have led to significant gains in cross-Departmental relationships, particularly at the operational level, but significant differences still remain. These differences can hinder effective decision-making and accountability.

For many of its early years, DHS did not have mature strategic planning, resource allocation, execution oversight, and reporting processes. The QHSR was a major milestone in the Department's strategic planning process; it has demonstrated both internally and externally the value of strategic planning and that strategic planning is possible within the homeland security mission space. The last few years have seen increased maturity in resource allocation and

execution oversight, particularly acquisition oversight. The Department has also systematically improved its financial management by building a strong internal controls process and focusing attention on the elimination of material weaknesses in financial audits.

#### *Congressional Accountability*

As the 9/11 Commission noted in its report, "Congress needs to establish for the Department of Homeland Security the kind of clear authority and responsibility that exist to enable ... the Defense Department to deal with threats to national security." Both the House and Senate Appropriations committees have consolidated all DHS jurisdiction into a single subcommittee within each chamber. Each chamber has also designated one authorization committee with primary oversight over DHS. However, DHS has had 86 committees and subcommittees exercising jurisdiction over the Department in each session of Congress since 2003. As a result, to date in the 111<sup>th</sup> Congress, DHS has provided testimony in more than 200 hearings from more than 280 Department witnesses. Over the past year, DHS provided approximately 5,227 Congressional briefings, formal and informal. A diagram of Congressional oversight of DHS in the 110th Congress is attached as Annex F. Streamlining Congressional oversight of DHS would allow the Department to focus its time and resources much more effectively on its critical missions, while preserving a full degree of accountability to Congress.

#### *Initiatives and Enhancements*

The QHSR established a foundation that will permit more effective and targeted analysis of DHS mission effectiveness. The QHSR legislation also required a review and assessment of the effectiveness of the mechanisms of the Department for executing the process of turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan within the Department. DHS conducted this analysis. DHS does not have a common analytic framework like that of the Department of Defense, which facilitates cross-Departmental planning and capability development. DHS will establish a common framework to effectively identify and assess alternatives and support decision-making at all levels. Additionally, the performance metrics that flow from department-wide analysis must be a priority for further development and refinement, both at the strategic and program levels. Lastly, though the Cost Analysis Division is an important step in the department's improved acquisition oversight, there remains a vital need for independent cost assessments of major programs. These initiatives are intended to improve the effectiveness of the mechanisms of the Department for executing the process of turning the requirements developed in the QHSR into an acquisition strategy and expenditure plan within the Department.

- *Increase Analytic Capability and Capacity.* Increasing the Department's analytic capability and capacity will help Department leadership better understand the implications of major decisions and the costs of alternative actions. DHS will enhance its strategic planning processes, resource allocation processes, risk analyses, net assessments, modeling capabilities, statistical analyses, and data collection in order to effectively project capability and capacity requirements for DHS missions and functions. DHS will take steps to develop common analytic frameworks and assumptions for use in cross-Departmental analysis, similar to the Department of Defense's Analytic Agenda

initiative. DHS will also reform its budget account structure to increase its ability to compare like costs across components and offices. As these reforms take shape, DHS will seek Congressional approval to conform its appropriations structure to this reformed account structure.

- *Improve Performance Measurement and Accountability.* Along with increased analytic capability and capacity, the Department must increase the quality of its performance measures and link those measures to the mission outcomes articulated in the QHSR Report. DHS has been actively working with the Government Accountability Office to address shortfalls in its current program performance measures, and the QHSR strategic framework provides the foundation upon which to base new strategic outcomes and measures. To that end, the Department will adjust its program-level performance measures, and introduce new strategic-level performance measures for cross-Departmental missions and functions. DHS will also expand program evaluation during and after program execution.
- *Strengthen Acquisition Oversight.* DHS has made significant improvements in acquisition oversight in the last two years; however, the Department needs to continue to strengthen this process. Numerous audits conducted by the Government Accountability Office and DHS Inspector General have highlighted significant program cost growth and the inadequacy of the cost estimating process across DHS. DHS has established a Cost Analysis Division (CAD) in the Office of the Chief Procurement Officer. Currently, the CAD is responsible for validating Program Life Cycle Cost Estimates. As a next step in its acquisition oversight process, DHS proposes to increase CAD's capability to provide independent cost estimates of major programs at major milestone points. This capability will ensure program cost estimates are reasonable reflections of the program's requirements and can withstand the scrutiny of external reviews and audits. Reliable and credible independent cost estimates will increase the Department's capability for informed investment decision making, budget formulation, progress measurement and accountability. Rigorous analyses of operational requirements, technology alternatives and disciplined testing and evaluation of technology acquisitions will be instituted to ensure investments yield intended mission improvements.

## VI. Conclusion

The Quadrennial Homeland Security Review, consistent with the *National Security Strategy*, was the first step in setting forth the strategic foundation to guide the activities of the homeland security enterprise toward a common end. This BUR report represents a second, DHS-focused step, and comprehensive effort to align the Department's programmatic activities and organizational structure with the mission sets and goals identified in the QHSR. The BUR serves as a road map for areas where additional emphasis, investment, and effort are needed to strengthen mission performance, improve Departmental operations and management and increase accountability for the resources entrusted to DHS.

The final step will be to execute the BUR. The BUR and QHSR will be implemented in the DHS FY 2012-2016 Future Years Homeland Security Program to Congress, which will propose

specific programmatic adjustments based on the BUR recommendations. DHS will also undertake, in coordination with appropriate interagency partners, additional efforts in support of the QHSR, including the development of requirements for intelligence, science and technology, support to civil authorities, and other elements described in this report. Together, the QHSR, the bottom-up review, and the budget proposals will serve as vital steps in maturing DHS into a truly strategy-driven organization.

As noted in the QHSR, the over-arching message is clear: this is a strong and resilient Nation, but one that must consistently adjust to an ever-changing threat environment. There are many critical roles to play—at DHS, across the Federal government, in Congress, throughout State, local, tribal, and territorial governments, within the private sector, and by families and in communities across the Nation. Through the commitment of each, we will secure the homeland for all.

**Annex A**  
**DHS Component Composition**

The Department of Homeland Security has a dynamic and complex mission and continually evaluates its force needs to optimally secure the homeland. The current composition of DHS forces is provided below. The QHSR and BUR results will be implemented in the FY 2012-2016 Future Years Homeland Security Program (FYHSP), which may drive additional changes. (Employee numbers are rounded)

***Transportation Security Administration (TSA):***

Headquarters and Supporting Resources  
     Operations Coordination Center  
     HQ Intelligence Office and Field Intelligence Officers  
     TSA Representation (19 countries)  
     Vetting and Credentialing Centers (primary and Back-up) (2)  
     Federal Flight Deck Officer Training Facilities (2)  
 Airport Passenger and Baggage Screening Operations (450 Airports)  
     Transportation Security Officers (45,000)  
     Behavior Detection Officers (3,000)  
     Bomb Appraisal Officers (400)  
     Canine Teams (165 Proprietary; 640 Agreements)  
 In-Flight Air Security  
     Federal Air Marshal Service  
 Surface and Multi-Modal Security  
     Multi-Modal Visible Intermodal Prevention and Response Teams (VIPR) (10)  
     Surface Transportation VIPR Teams (15)

***U.S. Customs and Border Protection (CBP):***

Headquarters and Supporting Resources  
 Air, Land, and Sea Ports of Entry (327)  
     Process Passengers and Pedestrians  
     CBP Officers (21,000)  
     Agricultural Specialists (2,000)  
 Border Security between Ports of Entry  
     20 Border Patrol sectors with 139 stations  
     Border Patrol Agents (20,000)  
 Air and Marine Operations (46 Air Units and 67 Marine Units)  
     Air Interdiction Agents (800)  
     Marine Interdiction Agents (350)  
 Assets  
     Aircraft (290)  
     Marine Vessels (235)

***U.S. Citizenship and Immigration Service (USCIS):***

## Headquarters and Supporting Resources

## Immigration Benefits Processing

District Offices providing adjudication of applications and petitions (26)

Service Center Operations (4)

Asylum Offices providing adjudication of asylum applications (8 domestic offices)

Refugee Offices providing adjudication of refugee applications (over 70 global offices)

International Operations (30 field offices)

Application Support Centers (129)

## Citizen Outreach

Information Call Centers

## Fraud Detection and National Security

Immigration Officers vetting of fraud and national security concerns (650)

***U.S. Immigration and Customs Enforcement (ICE):***

## Headquarters and Supporting Resources

## Office of Investigations

Special Agents in Charge Offices (SACS) (26)

Criminal Investigators (6,600)

## Office of Detention and Removal Operations

Field Office Directors (27)

Detention Officers (7,200)

Detention Beds (33,000)

## Office of the Principal Legal Advisor

Division Chiefs (13)

Chief Counsel (26)

Attorneys (851)

## Office of International Affairs

Attaché/Assistant Attaché Offices (63)

Special Agents (337)

Deportation Liaison Officers/ Detention &amp; Deportation Officer (1801) (18)

Intelligence Research Specialists/Analysts (4)

Foreign Service Nationals (118)

## Office of Professional Responsibility

Special Agents in Charge Offices (5)

Office locations nationwide (24)

Special Agents (323)

## Office of Intelligence

Field Intelligence Directors (26)

Special Agents (66)



***U.S. Secret Service (USSS):***

## Headquarters and Supporting Resources

Headquarters Divisions/Offices (30)

Administrative, Professional, and Technical Personnel (1,800)

## Protection and Investigations

Permanent Protective Details (8)

Special Agents (3,500)

Uniformed Division Officers (1,400)

Domestic Offices (116)

Foreign Offices (20)

***Federal Emergency Management Agency (FEMA):***

## Workforce

A blended workforce of 16,590 with 4,200 permanent, 3,390 temporary and 9,000 reserve employees

## Headquarters and Supporting Resources (1,988: 1,539 perm; 382 temp; 67 reserve)

Mount Weather Emergency Operations Center (837: 669 perm; 166 temp; 2 reserve)

## National Emergency Training Center (NETC) training facility (243), includes:

Emergency Management Institute (EMI) (58 perm; 15 temp; 9 reserve)

National Fire Academy (NFA) (110 perm; 1 temp)

Center for Domestic Preparedness (CDP) training facility (50 perm)

## Regional offices (10) and Area Offices (3)

Region 1 (100 perm; 17 temp; 570 reserve)

Region 2 (107 perm; 10 temp; 608 reserve)

Region 3 (101 perm; 14 temp; 519 reserve)

Region 4 (156 perm; 91 temp; 1311 reserve)

Region 5 (126 perm; 17 temp; 439 reserve)

Region 6 (126 perm; 85 temp; 912 reserve)

Region 7 (97 perm; 58 temp; 446 reserve)

Region 8 (89 perm; 20 temp; 433 reserve)

Region 9 (126 perm; 22 temp; 473 reserve)

Region 10 (97 perm; 15 temp; 585 perm)

Texas Transitional Recovery Office (1 temp)

Louisiana Transitional Recovery Office (1 perm; 485 temp)

Mississippi Transitional Recovery Office (276 temp)

## Disaster Reservists (9,000)

## Disaster Support Resources

National Response Coordination Center (NRCC) (1)

Regional Response Coordination Centers (RRCC) (10)

Federal Coordinating Officers (FCO) (1 perm; 37 temp)

National Incident Management Assistance Teams (IMAT) (2)

Regional Incident Management Assistance Teams (IMAT) (4)

Mobile Emergency Response Support (MERS) Detachments (6), each comprised of:

MERS Operations Centers (MOC)

Incident Response Vehicle (IRV) capability  
 Mobile Emergency Operations Vehicle (MEOV) capability  
 Forward Communications Vehicle (FCV) capability  
 Logistics Distribution Centers (8)  
 Mobile Disaster Recovery Centers (MDRC) (60)

***U.S. Coast Guard (USCG):***

Workforce  
 A blended work force with 50,720 active duty and reserve military members, 7,773 civilians, and over 30,000 volunteer members of the Auxiliary.

Support Commands  
 Coast Guard Headquarters, 2 Area Commands, 9 District Offices, 6 Logistics and Service Centers

Training Centers  
 6 Major Training Centers: Accession programs for cadets, officer candidates and new recruits and specialized training for Coast Guard job performance.

Shore-Based Multi-Mission Forces  
 35 Sector Commands with broad maritime safety and security authorities  
 945 air and marine stations throughout the United States with 1,850 small boats.

Deployable Forces  
 1 Maritime Security Response Team, 12 Maritime Safety and Security Teams, 8 Port Security Units, 17 Law Enforcement Detachments, 3 Strike Teams

Air and Maritime Fleet  
 43 Major Cutters, 30 Buoy Tenders, 121 Patrol Boats, 9 Domestic Icebreakers, 3 Polar Icebreakers.  
 143 Rotary Wing Aircraft, 56 Fixed Wing Aircraft

**Annex B****A Day in the Life of the Department of Homeland Security**

The Department of Homeland Security uses many tools and areas of expertise to accomplish our goal of securing the homeland. On any given day, we perform a variety of different tasks and functions to make America safer and our citizens more secure. Although our responsibilities are varied, we are united in a common purpose - 24 hours a day, 7 days a week. Below is a sampling of what the men and women of DHS do in a typical day. (All numbers are approximate averages.)

**Transportation Security Administration will:**

- Screen 2 million passengers and their 1.8 million pieces of checked baggage before they board commercial aircraft
- Intercept 2,000 prohibited items from people and carry-on baggage including 1,200 knives, blades or other sharp objects and 2 firearms
- Operate the National Explosives Detection Canine Team Program, which has 705 explosive detection canine teams deployed across the country
- Deploy thousands of Federal Air Marshals to protect flights in the United States and around the world
- Oversee screening of approximately seven million pounds per day of air cargo on domestic planes
- Conduct 4-5 Visible Intermodal Protection and Responses operations per day in passenger rail and mass transit systems somewhere in the United States

**U.S. Customs and Border Protection will:**

- Process over 1 million passengers and pedestrians
- Inspect nearly 60,000 truck, rail and sea containers
- Process \$88 million in fees, duties and tariffs
- Make 2,200 apprehensions between ports for illegal entry
- Seize 6,600 pounds of narcotics
- Seize 4,300 prohibited agricultural items
- Make 5,400 pre-departure seizures of prohibited agricultural items

**U.S. Citizenship and Immigration Services will:**

- Naturalize 2,900 new immigrants
- Conduct 135,000 national security background checks
- Process 27,400 applications for immigrant benefits
- Issue 7,200 permanent resident cards (green cards)
- Capture 8,700 sets of fingerprints at 130 Application Support Centers
- Welcome 3,200 new citizens and 3,300 new permanent residents
- Adjudicate nearly 200 refugee applications from around the world
- Grant asylum to 40 individuals already in the United States

**U.S. Immigration and Customs Enforcement will:**

- Make 63 administrative arrests and 89 criminal arrests
- Make 11 currency seizures totaling \$1.1 million

- Participate in 26 drug seizures each day, totaling 7,200 lbs. of marijuana, 7 lbs. of heroin, and 960 lbs. of cocaine
- ICE attorneys litigate 1,500 cases in immigration court and obtain 740 final orders of removal; 90 of those final orders of removal are for criminal aliens
- Screen 3,800 VISA applications
- House 29,800 illegal aliens in facilities nationwide

**United States Secret Service will:**

- Protect dozens of high profile government officials including the President, the Vice President, visiting heads of state, and former Presidents
- Seize \$319,000 in counterfeit currency and suppress a counterfeit operation
- Open 30 new financial crimes and counterfeit investigations and conduct 26 computer forensic examinations
- Seize \$300,000 in assets
- Arrest 25 individuals
- Conduct 8 public education seminars on counterfeit recognition and financial fraud schemes

**Federal Emergency Management Agency will:**

- Obligate \$39 million for disaster response, recovery, and mitigation activities
- Help save \$2.7 million in damages from flooding across the country through FEMA's Flood Plain Management
- Help protect an additional 104 homes from the devastating effects of flooding through flood insurance policies issued by the National Flood Insurance Program
- Provide \$181,000 for Fire Management Assistance grants, which aid state and local efforts in the suppression of wildfires
- Provide 11,300 publications through FEMA's U.S. Fire Administration to educate citizens about how to stay safe from fire and help America's fire service to safely respond to fires and other emergency incidents
- Arrange for translation services for disaster victims in up to 173 different languages through the National Processing Service Centers in Maryland, Puerto Rico, Texas and Virginia

**United States Coast Guard will:**

- Save 13 lives, respond to 64 search and rescue cases and prevent loss of \$260,000 in property damage
- Seize or remove 1,100 pounds of illegal drugs, with a street value of \$19 million
- Interdict 10 migrants attempting to illegally enter the United States via maritime routes
- Conduct 135 armed waterborne patrols projecting presence near maritime critical infrastructure and key resources
- Conduct 57 inspections of U.S. Flagged Vessels and safety exams on commercial fishing vessels
- Conduct 67 container inspections, and investigate and respond to 10 pollution incidents
- Issue 200 credentials to qualified merchant mariners to ensure the safety, security and efficiency of the maritime supply chain

- Perform 47 safety, security and environmental protection inspections at maritime facilities
- Ensure compliance with U.S. and foreign ships with international and U.S. shipboard air emission standards by conducting 32 exams
- Manage 3,500 commercial vessel transits through the Marine Transportation System to facilitate the safe and efficient movement of goods and people
- Provide reliable visual aids to navigation throughout the United States and its territories
- Conduct 14 fisheries boardings to ensure compliance with fisheries and marine protected species regulations
- Provide forces and capabilities to the Department of Defense to carry out U.S. national security objectives

**National Protection and Programs Directorate will:**

- Protect U.S. information systems through the United States Computer Emergency Readiness Team (US-CERT) by monitoring Federal Executive Branch civilian networks to identify emerging threats, ongoing trends, and intrusions; US-CERT detects and responds to an average of 64 incidents and 3,750 alert events daily
- Disrupt potential terrorist planning activities by conducting 5 Buffer Zone Protection assessments with local law enforcement at critical infrastructure and key resources in every sector across the Nation
- Analyze biometrics data on 100,000 foreign visitors and compare to the Federal watch list of 3.2 million known or suspected terrorists, criminals and immigration violators
- Identify 40 criminal migrants illegally attempting to enter the United States from the sea with biometric data and, through a partnership with the FBI, provide that information to state and local law enforcement agencies
- Use computer modeling and risk analysis to support critical decisions across the Department and to help the Nation prevent, protect, respond, and recover from all hazards
- Prevent 2,100 prohibited items from entering Federal facilities

**Science and Technology Directorate will:**

- Lead 200 projects to provide solutions to protect us from chemical, biological, and explosive attacks, provide security for our borders and shores, protect key parts of our infrastructure, and mitigate the effects of natural disasters.
- Assess 22 technology companies for product applicability to first responder customers, develop standards for first responder technologies to ensure high quality transitions, and provide test and evaluation services for DHS.

**Office of Operations Coordination and Planning (OPS) will:**

- Integrate department and interagency strategic level planning and operations coordination across the spectrum of prevent, protect, respond and recover
- Provide DHS with a joint operations coordination and planning capability at the strategic level to support internal DHS operational decision-making and Department leadership and participation in interagency operations
- Provide situational awareness and a common operating picture for the entire Federal government, and for State, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster

- Ensure that critical terrorism and disaster-related information reaches government decision-makers

**Management Directorate will:**

- Hire and process 100 new employees through its human capital office
- Obligate \$142 million through its finance office
- Issue 300 contracts through its procurement operations

**Office of Intelligence and Analysis will:**

- Review all-source intelligence information and produce analysis to distribute to Federal, State, local, tribal, territorial, and private sector partners regarding current and developing threats and vulnerabilities, as well as providing recommendations for potential protective measures

**Domestic Nuclear Detection Office will:**

- Provide radiation detection equipment to U.S. Customs and Border Protection to scan 70,000 cargo containers for radiological/nuclear material
- Train 12 State and local law enforcement officials on how to use preventive radiological/nuclear detection equipment

**Federal Law Enforcement Training Center will:**

- Train 3,500 Federal officers and agents from more than 80 different Federal agencies, as well as state, local, tribal and international officers and agents, in one or more of the 400 basic and advanced training programs available

**Office of Health Affairs will:**

- Retrieve samples from hundreds of BioWatch collectors that have been testing the air in our major metropolitan areas for evidence of biological pathogens
- Screen 350 sources of information from across multiple agencies and venues and assess them for significance and early recognition of a potential bio-event of national significance through the 24 hour watch of the National Biosurveillance Integration Center

**Office of Policy will:**

- Develop DHS-wide policies, programs, and planning to promote and ensure quality, consistency, and integration across all homeland security missions
- Provide thought leadership and analysis to the Secretary and other Departmental leaders to facilitate decision-making
- Represent the consolidated DHS position at White House interagency policy committee meetings
- Develop and articulate the long-term strategic view of the Department and translate the Secretary's strategic priorities into capstone planning products that drive increased operational effectiveness through integration, prioritization, and resource allocation
- Lead departmental international engagement
- Serve as a single point of contact for experts in academia, the private sector, and other external stakeholders to allow for streamlined policy development and management across the Department

**Annex C**  
**The DHS Efficiency Review**

The DHS Efficiency Review has focused on improvements regarding physical assets, workforce support, and day-to-day operations. A summary of Efficiency Review and related initiatives is set forth below.

Physical Assets

Strategic refinements in how DHS manages its physical assets have led to savings and improvements. For example, by using excess information technology equipment instead of buying new equipment, DHS has, to date, avoided costs of nearly \$3.9 million.

In the area of fleet management, DHS components are making great strides towards increasing the percentage of hybrids and alternative-fuel vehicles in their fleets. Components are also taking steps to encourage the use of alternative fuel instead of petroleum whenever possible.

Initiatives in this area include:

- Implementing an electronic tracking tool for fleet usage data to identify opportunities for alternative fuel usage; heighten vigilance for fraud, waste or abuse; and optimize fleet management;
- Initiating acquisition/leasing of hybrid vehicles for administrative use and alternative-fuel vehicles in cases where hybrids are not feasible;
- Implementing energy efficiencies in all facility management projects; and
- Utilizing wherever possible refurbished IT equipment (computers and mobile devices) and redeploying the current inventory throughout DHS.

Workforce Support

Supporting our workforce by giving them the tools and training they need is good business, and it translates into a more productive and efficient workforce.

Efficiency Review and other initiatives in this area include:

- Identifying and implementing Department-wide strategies to develop and retain our talented workforce, such as providing leadership training to emerging leaders;
- Developing cross-component training opportunities for employees;
- Establishing *Idea Factory* across the Department to encourage all DHS employees to contribute and rate ideas for improved operations;

- Establishing an employee resilience program to help identify and reduce sources of extreme job stress and promote employee wellness;
- Working aggressively to reduce the Department's reliance on contractors and contract services, in turn strengthening our Federal workforce;
- Standardizing content for new-employee orientation and mandatory annual training modules DHS-wide; and
- Focusing on achieving greater diversity in the leadership ranks of the Department.

#### Day-to-Day Operations

Changing the way the Department allocates resources, from acquiring office supplies to renting facilities, has allowed DHS to significantly reduce those costs. To date, DHS has avoided over \$35 million in costs through improved travel and conference planning. In addition, DHS expects to avoid costs of \$2.1 million in fiscal year 2010 by consolidating subscriptions for several publications, as well as \$138 million in software licensing and maintenance costs over the next six years.

Initiatives in this area include:

- Consolidating subscriptions to professional publications and newspapers and reducing the number of hard copies received by providing online access whenever possible;
- Maximizing the use of government office space for meetings and conferences in place of renting facilities;
- Minimizing the physical printing and distribution of reports and documents that can be sent electronically or posted online;
- Leveraging buying power to acquire software licenses for Department-wide usage;
- Eliminating non-mission critical travel and maximizing use of conference calls and web-based training and meetings;
- Increasing usage of DHS-wide blanket purchase agreements for office supplies; and
- Converting printers, fax machines, copiers, and scanners into all-in-one machines as replacements are needed.

In addition, DHS employees submitted thousands of suggestions in response to the President's SAVE award campaign. Many of these suggestions will be incorporated into the Efficiency Review initiatives in the coming year.



**Annex D****Alignment of Major DHS Programs to Homeland Security Missions**

In addition to developing the initiatives discussed in the main text of this document, the bottom-up review also conducted a detailed examination of DHS activities and the alignment of these activities to the QHSR mission areas and other complementary Departmental responsibilities for which DHS develops hybrid capabilities. This will facilitate a detailed evaluation of what DHS does within each mission area and identify gaps and overlaps within and across mission areas. This work is also building a foundation for a unified programmatic structure and strategic architecture. This work is ongoing. To provide a view of preliminary alignment, a high-level summary of selected major categories from DHS's existing program structure is shown below. Also shown is a preliminary alignment of DHS's major investments with each mission. Note that while many of these programs and investments cut across multiple mission areas, for display purposes only one alignment is shown.

**Preventing Terrorism and Enhancing Security:**

- Major FYHSP Programmatic Activity:
  - Aviation Security (TSA)
  - Surface Transportation Security (TSA)
  - Federal Air Marshal Service (TSA)
  - Transportation Threat Assessment and Credentialing (TTAC) (TSA)
  - Domestic Protectees (USSS)
  - Protective Intelligence (USSS)
  - Campaign Protection (USSS)
  - Foreign Protectees and Foreign Missions (USSS)
  - Infrastructure Protection (USSS)
  - Infrastructure Protection (NPPD)
  - Federal Protective Service (NPPD)
  - Domestic Nuclear Detection (DNDO)
  - Medical and Biodefense (OHA)
  - Chemical and Biological Research and Development (S&T)
  - Radiological and Nuclear Research and Development (S&T)
  - Ports, Waterways and Coastal Security (USCG)
- Major Acquisitions and Investments:
  - Electronic Baggage Screening Program (TSA)
  - Passenger Screening Program (TSA)
  - Secure Flight (TSA)
  - Transportation Worker Identification Credentialing (TSA)
  - Advance Spectroscopy Portals (DNDO)
  - Cargo Advanced Automated Radiography System (DNDO)
  - Infrastructure Information Collection and Visualization (NPPD)

**Securing and Managing our Borders:**

- Major FYHSP Programmatic Activity:
  - Border Security and Control between Ports of Entry (CBP)
  - Border Security Inspections and Trade Facilitation at Ports of Entry (CBP)

- Border Security Fencing, Infrastructure, and Technology (CBP)
- Air and Marine (CBP)
- Automation Modernization (CBP)
- Drug Interdiction (USCG)
- Migrant Interdiction (USCG)
- US-VISIT (NPPD)
- Border and Maritime Security Research and Development (S&T)
- Major Acquisitions and Investments:
  - Strategic Air and Marine Plan (CBP)
  - Secure Border Initiative Net (CBP)
  - Border Patrol Facilities (CBP)
  - Non-Intrusive Inspection Systems Program (CBP)
  - Traveler Enforcement Compliance System Modernization (CBP)
  - Secure Border Initiative Tactical Infrastructure (CBP)
  - EWP Tactical Communications (CBP)
  - License Plate Reader (CBP)
  - Automated Commercial Environment / International Trade Data System (CBP)
  - Electronic System for Travel Authorization (CBP)
  - Secure Freight Initiative (CBP)
  - Advance Passenger Information System (CBP)
  - Western Hemisphere Travel Initiative (CBP)
  - Automated Targeting System (CBP)
  - Offshore Patrol Cutter (USCG)
  - National Security Cutter (USCG)
  - HC-130 Conversion/Sustainment Project (USCG)
  - HH-65 Conversion/Sustainment Project (USCG)
  - HC-144A Maritime Patrol Aircraft (USCG)
  - Medium Endurance Cutter Sustainment (USCG)
  - Fast Response Cutter - B class (USCG)
  - Nationwide Automation Identification System (USCG)
  - HH-60 Conversion/Sustainment Project (USCG)
  - Unmanned Aircraft Systems (USCG)
  - Patrol Boat Sustainment (USCG)
  - HC-130J Fleet Introduction (USCG)
  - Response Boat – Medium (USCG)
  - United States Visitor and Immigrant Status Indicator Technology (NPPD)
  - ATLAS (ICE)

**Enforcing and Administering our Immigration Laws:**

- Major FYHSP Programmatic Activity:
  - Adjudication Services (USCIS)
  - Information and Customer Service (USCIS)
  - Citizenship (USCIS)
  - Immigration Status Verification (USCIS)
  - Immigration Security and Integrity (USCIS)
  - Investigations (ICE)

- Detention and Removal Operations (ICE)
- Automation Modernization (ICE)
- International Affairs (ICE)
- Migrant Interdiction (USCG)
- Major Acquisitions and Investments:
  - Transformation (USCIS)
  - Integrated Document Production (USCIS)
  - Verification Information System / Employment Eligibility Verification (USCIS)
  - Detention and Removal Modernization (ICE)

**Safeguarding and Securing Cyberspace:**

- Major FYHSP Programmatic Activity:
  - Cyber Security and Communications (NPPD)
- Major Acquisitions and Investments:
  - Homeland Security Information Network (AO)
  - Homeland Secure Data Network (DHS)
  - National Cybersecurity and Protection System (NPPD)
  - Information Systems Security (NPPD)

**Ensuring Resilience to Disasters:**

- Major FYHSP Programmatic Activity:
  - Mitigation (FEMA)
  - National Preparedness (FEMA)
  - Disaster Operations (FEMA)
  - Disaster Assistance (FEMA)
  - Logistics Management (FEMA)
  - U.S. Fire Administration (FEMA)
  - National Continuity Programs (FEMA)
  - Search and Rescue (USCG)
- Major Acquisitions and Investments:
  - BioWatch Gen-3 (OHA)
  - National Bio and Agro-Defense Facility (S&T)
  - National Biodefense Analysis and Countermeasures Center Facility (S&T)
  - Risk Mapping, Analysis and Planning (FEMA)
  - Housing Inspection Services (FEMA)
  - Risk Mapping, Analysis and Planning IT (FEMA)
  - Total Asset Visibility (FEMA)
  - C4ISR – COP (USCG)
  - Interagency Operations Centers (Command 21) (USCG)
  - Rescue 21 (USCG)

**Complementary Departmental Responsibilities and Hybrid Capabilities**

As noted above, DHS also performs a number of services and functions that are complementary to its homeland security mission responsibilities, including marine safety, stewardship, and environmental protection and certain categories of law enforcement activities. These services

and functions are typically performed with hybrid capabilities—assets and resources capable of performing multiple missions—which are a hallmark of homeland security. For example, the same assets and personnel that patrol our borders, enforce our immigration laws, and respond to major oil spills also enforce safety regulations, assist travelers, and safeguard natural resources. These complementary activities are critical to fulfilling other national interests, and are often intertwined with and mutually supporting of homeland security activities. Some of these activities include the following:

- Major FYHSP Programmatic Activity:
  - Marine Environmental Protection (USCG)
  - Marine Safety (USCG)
  - Other Law Enforcement (USCG)
  - Living Marine Resources (USCG)
  - Search and Rescue (USCG)
  - Defense Readiness (USCG)
  - Waterways Management: Aids to Navigation (USCG)
  - Waterways Management: Ice Operations (USCG)
  - Financial Investigations (USSS)

As the Department continues to evaluate its inventory of activities, it will gain increased insight into those Departmental activities that are complementary to its homeland security mission responsibilities but remain vital and continue to be performed most effectively and efficiently by DHS. This additional breakout will be provided in the President's FY 2012 Budget and the accompanying FY 2012-2016 Future Years Homeland Security Program.

**Annex E**  
**Sector-Specific Agencies**  
*(Source: National Infrastructure Protection Plan)*

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture (a)	Agriculture and Food
Department of Health and Human Services (b)	
Department of Defense (c)	Defense and Industrial Base
Department of Energy	Energy (d)
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water (e)
Department of Homeland Security	Chemical
Office of Infrastructure Protection	Commercial Facilities
	Critical Manufacturing
	Dams
	Emergency Services
	Nuclear Reactors, Materials, and Waste
	Government Facilities (g)
Office of Cybersecurity and Communications	Information Technology
Transportation Security Administration	Communications
Transportation Security Administration	Postal and Shipping
United States Coast Guard (f)	Transportation Systems (h)

- a The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).  
b The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.  
c Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DOD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.  
d The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.  
e The Water Sector includes drinking water and wastewater systems.  
f The U.S. Coast Guard is the SSA for the maritime transportation mode.  
g The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector.  
h As stated in HSPD-7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to transportation security and transportation infrastructure protection.

**Annex F**  
**Congressional Oversight of DHS in the 110th Congress**

